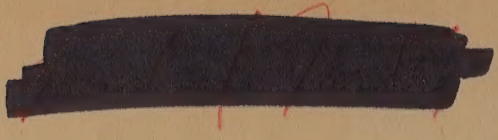

150

BERTRAND SMITH'S
"ACRES OF BOOKS"
633 MAIN ST.

MATHEMATICAL MONOGRAPHS

EDITED BY

THE LATE MANSFIELD MERRIMAN

AND

THE LATE ROBERT S. WOODWARD

Octavo, Cloth

No. 1. History of Modern Mathematics. (Out of Print)
By DAVID EUGENE SMITH.

No. 2. Synthetic Projective Geometry. (Out of Print)
By the Late GEORGE BRUCE HALSTED.

No. 3. Determinants.
By the Late LAENAS GIFFORD WELD.

No. 4. Hyperbolic Functions. (Out of Print)
By the Late JAMES MCMAHON.

No. 5. Harmonic Functions. (Out of Print)
By the Late WILLIAM E. BYERLY.

No. 6. Grassmann's Space Analysis. (Out of Print)
By EDWARD W. HYDE.

No. 7. Probability and Theory of Errors. (Out of Print)
By the Late ROBERT S. WOODWARD.

No. 8. Vector Analysis and Quaternions.
By the Late ALEXANDER MACFARLANE.

No. 9. Differential Equations.
By the Late WILLIAM WOOLSEY JOHNSON.

No. 10. The Solution of Equations.
By the Late MANSFIELD MERRIMAN.

No. 11. Functions of a Complex Variable. (Out of Print)
By THOMAS S. FISKE.

No. 12. The Theory of Relativity.
By ROBERT D. CARMICHAEL.

No. 13. The Theory of Numbers.
By ROBERT D. CARMICHAEL.

No. 14. Algebraic Invariants.
By LEONARD E. DICKSON.

No. 16. Diophantine Analysis.
By ROBERT D. CARMICHAEL.

No. 17. Ten British Mathematicians.
By the Late ALEXANDER MACFARLANE.

No. 18. Elliptic Integrals. (Out of Print)
By HARRIS HANCOCK.

No. 19. Empirical Formulas.
By THEODORE R. RUNNING.

No. 20. Ten British Physicists.
By the Late ALEXANDER MACFARLANE.

No. 21. The Dynamics of the Airplane. (Out of Print)
By KENNETH P. WILLIAMS.

PUBLISHED BY

JOHN WILEY & SONS, Inc., NEW YORK

CHAPMAN & HALL, Limited, LONDON

MATHEMATICAL MONOGRAPHS

EDITED BY

THE LATE MANSFIELD MERRIMAN AND
THE LATE ROBERT S. WOODWARD

No. 16

DIOPHANTINE ANALYSIS

BY

ROBERT D. CARMICHAEL,
DEAN OF GRADUATE SCHOOL AND PROFESSOR OF MATHEMATICS
IN THE UNIVERSITY OF ILLINOIS

NEW YORK
JOHN WILEY & SONS, INC.
LONDON: CHAPMAN & HALL, LIMITED

COPYRIGHT, 1915,
BY
ROBERT D. CARMICHAEL

PRINTED AND BOUND BY
BRAUNWORTH & CO., INC.
BUILDERS OF BOOKS
BRIDGEPORT, CONN.

2/41

PREFACE

THE author's purpose in writing this book has been to supply the reader with a convenient introduction to Diophantine Analysis. The choice of material has been determined by the end in view. No attempt has been made to include all special results, but a large number of them are to be found both in the text and in the exercises. The general theory of quadratic forms has been omitted entirely, since that subject would require a volume in itself. The reader will therefore miss such an elegant theorem as the following: Every positive integer may be represented as the sum of four squares. Some methods of frequent use in the theory of quadratic forms, in particular that of continued fractions, have been left out of consideration even though they have some value for other Diophantine questions. This is done for the sake of unity and brevity. Probably these omissions will not be regretted, since there are accessible sources through which one can make acquaintance with the parts of the theory excluded.

For the range of matter actually covered by this text there seems to be no consecutive exposition in existence at present in any language. The task of the author has been to systematize, as far as possible, a large number of isolated investigations and to organize the fragmentary results into a connected body of doctrine. The principal single organizing idea here used and not previously developed systematically in the literature is that connected with the notion of a multiplicative domain introduced in Chapter II.

The table of contents affords an indication of the extent and arrangement of the material embodied in the work.

Concerning the exercises some special remarks should be made. They are intended to serve three purposes: to afford practice material for developing facility in the handling of problems in Diophantine analysis; to give an indication of what special results have already been obtained and what special problems have been found amenable to attack; and to point out unsolved problems which are interesting either from their elegance or from their relation to other problems which already have been treated.

Corresponding roughly to these three purposes the problems have been divided into three classes. Those which have no distinguishing mark are intended to serve mainly the purpose first mentioned. Of these there are 133, of which 45 are in the Miscellaneous Exercises at the end of the book. Many of them are inserted at the end of individual sections with the purpose of suggesting that a problem in such position is readily amenable to the methods employed in the section to which it is attached. The harder problems taken from the literature of the subject are marked with an asterisk; they are 53 in number. Some of them will serve a disciplinary purpose; but they are intended primarily as a summary of known results which are not otherwise included in the text or exercises. In this way an attempt has been made to gather up into the text and the exercises all results of essential or considerable interest which fall within the province of an elementary book on Diophantine analysis; but where the special results are so numerous and so widely scattered it can hardly be supposed that none of importance has escaped attention. Finally those exercises which are marked with a dagger (35 in number) are intended to suggest investigations which have not yet been carried out so far as the author is aware. Some of these are scarcely more than exercises, while others call for investigations of considerable extent or interest.

ROBERT D. CARMICHAEL.

CONTENTS

CHAPTER I. INTRODUCTION. RATIONAL TRIANGLES. METHOD OF INFINITE DESCENT

PAGE

§ 1. Introductory Remarks 1
§ 2. Remarks Relating to Rational Triangles 8
§ 3. Pythagorean Triangles. Exercises 1–6 9
§ 4. Rational Triangles. Exercises 1–3 11
§ 5. Impossibility of the System $x^2+y^2=z^2$, $y^2+z^2=t^2$. Applications. Exercises 1–3 14
§ 6. The Method of Infinite Descent. Exercises 1–9 18
General Exercises 1–10 22

CHAPTER II. PROBLEMS INVOLVING A MULTIPLICATIVE DOMAIN

§ 7. On Numbers of the Form $x^2+axy+by^2$. Exercises 1–7 24
§ 8. On the Equation $x^2-Dy^2=z^2$. Exercises 1–8 26
§ 9. General Equation of the Second Degree in Two Variables 34
§ 10. Quadratic Equations Involving More than Three Variables. Exercises 1–6 35
§ 11. Certain Equations of Higher Degree. Exercises 1–3 44
§ 12. On the Extension of a Set of Numbers so as to Form a Multiplicative Domain 48
General Exercises 1–22 52

CHAPTER III. EQUATIONS OF THE THIRD DEGREE

§ 13. On the Equation $kx^3+ax^2y+bxy^2+cy^3=t^2$ 55
§ 14. On the Equation $kx^3+ax^2y+bxy^2+cy^3=t^3$ 57
§ 15. On the Equation $x^3+y^3+z^3-3xyz=u^3+v^3+w^3-3uvw$ 62
§ 16. Impossibility of the Equation $x^3+y^3=2^mz^3$ 67
General Exercises 1–26 72

CHAPTER IV. EQUATIONS OF THE FOURTH DEGREE

§ 17. On the Equation $ax^4+bx^3y+cx^2y^2+dxy^3+ey^4=mz^2$. Exercises 1–4 74
§ 18. On the Equation $ax^4+by^4=cz^2$. Exercises 1–4 77
§ 19. Other Equations of the Fourth Degree 80
General Exercises 1–20 83

CHAPTER V. EQUATIONS OF DEGREE HIGHER THAN THE FOURTH. THE FERMAT PROBLEM

PAGE

§ 20. Remarks Concerning Equations of Higher Degree 85
§ 21. Elementary Properties of the Equation $x^n+y^n=z^n$, $n>2$ 86
§ 22. Present State of Knowledge Concerning the Equation $x^p+y^p+z^p=0$ 100
General Exercises 1–13 102

CHAPTER VI. THE METHOD OF FUNCTIONAL EQUATIONS

§ 23. Introduction. Rational Solutions of a Certain Functional Equation 104
§ 24. Solution of a Certain Problem from Diophantus 106
§ 25. Solution of a Certain Problem Due to Fermat 108
General Exercises 1–6 111

MISCELLANEOUS EXERCISES 1–71 112

INDEX 117

DIOPHANTINE ANALYSIS

CHAPTER I

INTRODUCTION. RATIONAL TRIANGLES. METHOD OF INFINITE DESCENT

§ 1. Introductory Remarks

In the theory of Diophantine analysis two closely related but somewhat different problems are treated. Both of them have to do primarily with the solution, in a certain sense, of an equation or a system of equations. They may be characterized in the following manner: Let $f(x, y, z, \ldots)$ be a given polynomial in the variables $x, y, z, \ldots$ with rational (usually integral) coefficients and form the equation

$$f(x, y, z, \ldots) = 0.$$

This is called a *Diophantine equation* when we consider it from the point of view of determining the *rational* numbers $x, y, z, \ldots$ which satisfy it. We usually make a further restriction on the problem by requiring that the solution $x, y, z, \ldots$ shall consist of *integers*; and sometimes we say that it shall consist of positive integers or of some other defined class of integers. Connected with the above equation we thus have two problems, namely: To find the rational numbers $x, y, z, \ldots$ which satisfy it; to find the integers (or the positive integers) $x, y, z, \ldots$ which satisfy it.

Similarly, if we have several such functions $f_i(x, y, z, \ldots)$, in number less than the number of variables, then the set of equations

$$f_i(x, y, z, \ldots) = 0$$

is said to be a *Diophantine system* of equations.

Any set of rational numbers $x, y, z, \ldots$, which satisfies the equation [system], is said to be a *rational solution* of the equation [system]. An *integral solution* is similarly defined. The *general rational* [*integral*] *solution* is a solution or set of solutions containing all rational [integral] solutions. A *primitive solution* is an integral solution in which the greatest common divisor of the values of $x, y, z, \ldots$ is unity.

A certain extension of the foregoing definition is possible. One may replace the function $f(x, y, z, \ldots)$ by another which is not necessarily a polynomial. Thus, for example, one may ask what integers x and y can satisfy the relation

$$x^y - y^x = 0.$$

This more extended problem is all but untreated in the literature. It seems to be of no particular importance and therefore will be left almost entirely out of account in the following pages.

We make one other general restriction in this book; we leave linear equations out of consideration. This is because their theory is different from that of non-linear equations and is essentially contained in the theory of linear congruences.

That a Diophantine equation may have no solution at all or only a finite number of solutions is shown by the examples

$$x^2 + y^2 + 1 = 0, \quad x^2 + y^2 - 1 = 0.$$

Obviously the first of these equations has no rational solution and the second only a finite number of integral solutions. That the number of rational solutions of the second is infinite will be seen below. Furthermore we shall see that the equation $x^2 + y^2 = z^2$ has an infinite number of integral solutions.

In some cases the problem of finding rational solutions and that of finding integral solutions are essentially equivalent. This is obviously true in the case of the equation $x^2 + y^2 = z^2$. For, the set of all rational solutions contains the set of all integral solutions, while from the set of all integral solutions it is obvious that the set of all rational solutions is obtained by dividing the numbers in each solution by an

arbitrary positive integer. In a similar way it is easy to see that the two problems are essentially equivalent in the case of every homogeneous equation.

In certain other cases the two problems are essentially different, as one may see readily from such an equation as $x^2+y^2=1$. Obviously, the number of integral solutions is finite; moreover, they are trivial. But the number of rational solutions is infinite and they are not all trivial in character, as we shall see below.

Sometimes integral solutions may be very readily found by means of rational solutions which are easily obtained in a direct way. Let us illustrate this remark with an example. Consider the equation

$$x^2+y^2=z^2. \tag{1}$$

The cases in which x or y is zero are trivial, and hence they are excluded from consideration. Let us seek first those solutions in which z has the given value $z=1$. Since $x\neq 0$ we may write y in the form $y=1-mx$, where m is *rational*. Substituting in (1) we have

$$x^2+(1-mx)^2=1.$$

This yields

$$x=\frac{2m}{1+m^2};$$

whence

$$y=\frac{1-m^2}{1+m^2}.$$

This, with $z=1$, gives a *rational* solution of Eq. (1) for every rational value of m. (Incidentally we have in the values of x and y an infinite set of rational solutions of the equation $x^2+y^2=1$.)

If we replace m by q/p, where q and p are relatively prime integers, and then multiply the above values of x, y, z by p^2+q^2, we have the new set of values

$$x=2pq, \quad y=p^2-q^2, \quad z=p^2+q^2.$$

This affords a two-parameter *integral* solution of (1).

In § 3 we return to the theory of Eq. (1), there deriving the solution in a different way. The above exposition has

been given for two reasons: It illustrates the way in which rational solutions may often be employed to obtain integral solutions (and this process is frequently one of considerable importance); again, the spirit of the method is essentially that of the Greek mathematician Diophantus, who flourished probably about the middle of the third century of our era and who wrote the first systematic exposition of what is now known as Diophantine analysis. The reader is referred to Heath's *Diophantos of Alexandria* for an account of this work and for an excellent abstract (in English) of the extant writings of Diophantus.

The theory of Diophantine analysis has been cultivated for many centuries. As we have just said, it takes its name from the Greek mathematician Diophantus. The extent to which the writings of Diophantus are original is unknown, and it is probable now that no means will ever be discovered for settling this question; but whether he drew much or little from the work of his predecessors it is certain that his *Arithmetica* has exercised a profound influence on the development of number theory.

The bulk of the work of Diophantus on the theory of numbers consists of problems leading to indeterminate equations; these are usually of the second degree, but a few indeterminate equations of the third and fourth degrees appear and at least one easy one of the sixth degree is to be found. The general type of problem is to find a set of numbers, usually two or three or four in number, such that different expressions involving them in the first and second and third degrees are squares or cubes or otherwise have a preassigned form.

As good examples of these problems we may mention the following: To find three squares such that the product of any two of them added to the sum of those two or to the remaining one gives a square; to find three squares such that their continued product added to any one of them gives a square; to find two numbers such that their product plus or minus their sum gives a cube. (See Chapter VI.)

Diophantus was always satisfied with a rational result

even though it appeared in fractional form; that is, he did not insist on having a solution in integers as is customary in most of the recent work in Diophantine analysis.

It is through Fermat that the work of Diophantus has exercised the most pronounced influence on the development of modern number theory. The germ of this remarkable growth is contained in what is only a part of the original Diophantine analysis, of which, without doubt, Fermat is the greatest master who has yet appeared. The remarks, method and results of the latter mathematician, especially those recorded on the margin of his copy of Diophantus, have never ceased to be the marvel of other workers in this fascinating field. Beyond question they gave the fundamental initial impulse to the brilliant work in the theory of numbers which has brought that subject to its present state of advancement.

Many of the theorems announced without proof by Fermat were demonstrated by Euler, in whose work the spirit of the method of Diophantus and Fermat is still vigorous. In the *Disquisitiones Arithmeticæ*, published in 1801, Gauss introduced new methods, transforming the whole subject and giving it a new tendency toward the use of analytical methods. This was strengthened by the further discoveries of Cauchy, Jacobi, Eisenstein, Dirichlet, and others.

The development in this direction has extended so rapidly that by far the larger portion of the now existing body of number theory has had its origin in this movement. The science has thus departed widely from the point of view and the methods of the two great pioneers Diophantus and Fermat.

Yet the methods of the older arithmeticians were fruitful in a marked degree.* They announced several theorems which have not yet been proved or disproved and many others the proofs of which have been obtained by means of such difficulty as to make it almost certain that they possessed other and simpler methods for their discovery. Moreover they made a beginning of important theories which remain to this day in a more or less rudimentary stage.

* Cf. G. B. Mathews, *Encyclopaedia Britannica*, 11th edition, Vol. XIX, p. 863.

During all the intervening years, however, there has been a feeble effort along the line of problems and methods in indeterminate equations similar to those to be found in the works of Diophantus and Fermat; but this has been disjointed and fragmentary in character and has therefore not led to the development of any considerable body of connected doctrine. Into the history of this development we shall not go; it will be sufficient to refer to general works of reference * by means of which the more important contributions can be found.

Notwithstanding the fact that the Diophantine method has not yet proved itself particularly valuable, even in the domain of Diophantine equations where it would seem to be specially adapted, still one can hardly refuse to believe that it is after all the method which is really germane to the subject. It will of course need extension and addition in some directions in order that it may be effective. There is hardly room to doubt that Fermat was in possession of such extensions if he did not indeed create new methods of a kindred sort. More recently Lucas † has revived something of the old doctrine and has reached a considerable number of interesting results.

The fragmentary character of the body of doctrine in Diophantine anlysis seems to be due to the fact that the history of the subject has been primarily that of special problems. At no time has the development of method been conspicuous, and there has never been any considerable body of doctrine worked out according to a method of general or even of fairly general applicability. The earliest history of the subject has been peculiarly adapted to bring about this state of things. It was the plan of presentation of Diophantus to announce a problem and then to give a solution of it in the most convenient form for exposition, thus allowing the reader but small opportunity to ascertain how the author was led either to the problem or to its solution. The contributions of Fermat were

* See *Encyclopédie des sciences mathématiques*, tome I, Vol. III, pp. 27–38, 201–214; *Royal Society Index*, Vol. I, pp. 201–219.

† *American Journal of Mathematics*, Vol. I (1878), pp. 184, 289.

mainly in the form of results stated without proof. Moreover, through their correspondence with Fermat or their relation to him in other ways, many of his contemporaries also were led to announce a number of results without demonstration. Naturally there was a desire to find proofs of interesting theorems made known in this way. Thus it happened that much of the earlier development of Diophantine analysis centered around the solution of certain definite special problems or the demonstration of particular theorems.

There is also something in the nature of the subject itself which contributed to bring this about. If one begins to investigate problems of the character of those solved by Diophantus and Fermat he is soon led experimentally to observe certain apparent laws, and this naturally excites his curiosity as to their generality and possible means of demonstrating them. Thus one is led again to consider special problems.

Now when we attack special problems, instead of devising and employing general methods of investigation in a prescribed domain, we fail to forge all the links of a chain of reasoning necessary in order to build up a connected body of doctrine of considerable extent and we are thus lost amid our difficulties, because we have no means of arranging them in a natural or logical order. We are very much in the situation of the investigator who tries to make headway by considering only those matters which have a practical bearing. We do not make progress because we fail to direct our attention to essential parts of our problems.

It is obvious that the theory of Diophantine analysis is in need of general methods of investigation; and it is important that these, when discovered, shall be developed to a wide extent. In this book are gathered together the important results so far developed and a number of new ones are added. Many of the older ones are derived in a new way by means of two general methods first systematically developed in the present work. These are the method of the multiplicative domain introduced in Chapter II and the method of functional equations employed in Chapter VI. Neither of these methods

is here used to the full extent of its capacity; this is especially true of the latter. In a book such as the present it is natural that one should undertake only an introductory account of these methods.

§ 2. Remarks Relating to Rational Triangles

A triangle whose sides and area are rational numbers is called a *rational triangle*. If the sides of a rational triangle are integers it is said to be *integral*. If further these sides have a greatest common divisor unity the triangle is said to be *primitive*. If the triangle is right-angled it is said to be a *right-angled rational triangle* or a *Pythagorean triangle* or a *numerical right triangle*.

It is convenient to speak, in the usual language of geometry, of the hypotenuse and legs of the right triangle. If x and y are the legs and z the hypotenuse of a Pythagorean triangle, then

$$x^2+y^2=z^2.$$

Any rational solution of this equation affords a Pythagorean triangle. If the triangle is primitive, it is obvious that no two of the numbers x, y, z have a common prime factor. Furthermore, all rational solutions of this equation are obtained by multiplying each primitive solution by an arbitrary rational number.

From the cosine formula of trigonometry it follows immediately that the cosine of each angle of a rational triangle is itself rational. Hence a perpendicular let fall from any angle upon the opposite side divides that side into two rational segments. The length of this perpendicular is also a rational number, since the sides and area of the given triangle are rational. Hence every rational triangle is a sum of two Pythagorean triangles which are formed by letting a perpendicular fall upon the longest side from the opposite vertex. Thus the theory of rational triangles may be based upon that of Pythagorean triangles.

A more direct method is also available. Thus if a, b, c

are the sides and A the area of a rational triangle we have from geometry

$$(a+b+c)(-a+b+c)(a-b+c)(a+b-c)=16A^2.$$

Putting

$$a=\beta+\gamma, \quad b=\gamma+\alpha, \quad c=\alpha+\beta,$$

we have

$$(\alpha+\beta+\gamma)\alpha\beta\gamma=A^2.$$

Every rational solution of the last equation affords a rational triangle.

In the next two sections we shall take up the problem of determining all Pythagorean triangles and all rational triangles.

It is of interest to observe that Pythagorean triangles have engaged the attention of mathematicians from remote times. They take their name from the Greek philosopher Pythagoras, who proved the existence of those triangles whose legs and hypotenuse in modern notation would be denoted by $2\alpha+1$, $2\alpha^2+2\alpha$, $2\alpha^2+2\alpha+1$, respectively, where α is a positive integer. Plato gave the triangles 2α, α^2-1, α^2+1. Euclid gave a third set, while Diophantus derived a formula essentially equivalent to the general solution obtained in the following section.

Fermat gave a great deal of attention to problems connected with Pythagorean triangles, and it is not too much to say that the modern theory of numbers had its origin in the meditations of Fermat concerning these and related problems.

§ 3. Pythagorean Triangles

We shall now determine the general form of the positive integers x, y, z which afford a primitive solution of the equation

$$x^2+y^2=z^2. \tag{1}$$

The square of the odd number $2\mu+1$ is $4\mu^2+4\mu+1$. Hence the sum of two odd squares is divisible by 2 but not by 4; and therefore the sum of two odd squares cannot be a square. Hence of the numbers x, y in (1) one is even. If we suppose that x is even, then y and z are both odd.

Let us write Eq. (1) in the form

$$x^2=(z+y)(z-y). \tag{2}$$

Every common divisor of $z+y$ and $z-y$ is a divisor of their difference $2y$. Thence, since z and y are relatively prime odd numbers, we conclude that 2 is the greatest common divisor of $z+y$ and $z-y$. Then from (2) we see that each of these numbers must be twice a square, so that we may write

$$z+y=2a^2, \quad z-y=2b^2,$$

where a and b are relatively prime integers. From these two equations and Eq. (2) we have

$$x=2ab, \quad y=a^2-b^2, \quad z=a^2+b^2. \tag{3}$$

Since x and y are relatively prime, it follows that one of the numbers a, b is odd and the other even.

The forms of x, y, z given in (3) are necessary in order that (1) may be satisfied, while at the same time x, y, z are relatively prime and x is even. A direct substitution in (1) shows that this equation is indeed satisfied by these values. Hence we have the following theorem:

The legs and hypotenuse of any primitive Pythagorean triangle may be put in the form

$$2ab, \quad a^2-b^2, \quad a^2+b^2. \tag{4}$$

respectively, where a and b are relatively prime positive integers of which one is odd and the other even and a is greater than b; and every set of numbers (4) *forms a primitive Pythagorean triangle.*

If we take $a=2$, $b=1$, we have $4^2+3^2=5^2$; if $a=3$, $b=2$, we have $12^2+5^2=13^2$; and so on.

EXERCISES

1. Prove that the legs and hypotenuse of all integral Pythagorean triangles in which the hypotenuse differs from one leg by unity are given by $2\alpha+1$, $2\alpha^2+2\alpha$, $2\alpha^2+2\alpha+1$, respectively, α being a positive integer.

2. Prove that the legs and hypotenuse of all primitive Pythagorean triangles in which the hypotenuse differs from one leg by 2 are given by 2α, α^2-1, α^2+1, respectively, α being a positive integer. In what non-primitive triangles does the hypotenuse exceed one leg by 2?

3. Show that the product of the three sides of a Pythagorean triangle is divisible by 60.

4. Show that the general formulæ for the solution of the equation

$$x^2+y^2=z^4$$

in relatively prime positive integers x, y, z are

$$z=m^2+n^2, \quad x, y=4mn(m^2-n^2), \quad \pm(m^4-6m^2n^2+n^4), \quad m>n,$$

m and n being relatively prime positive integers of which one is odd and the other even.

5. Show that the general formulæ for the solution of the equation

$$x^2+(2y)^4=z^2$$

in relatively prime positive integers x, y, z are

$$z=4m^4+n^4, \quad x=\pm(4m^4-n^4), \quad y=mn,$$

m and n being relatively prime positive integers.

6. Show that the general formulæ for the solution of the equation

$$(2x)^2+y^4=z^2$$

in relatively prime positive integers x, y, z are

$$z=m^4+6m^2n^2+n^4, \quad x=2mn(m^2+n^2), \quad y=m^2-n^2, \quad m>n,$$

m and n being relatively prime positive integers of which one is odd and the other even.

§ 4. Rational Triangles

We have seen that the length of the perpendicular from any angle to the opposite side of a rational triangle is rational, and that it divides that side into two parts each of which is of rational length. If we denote the sides of the triangle by x, y, z, the perpendicular from the opposite angle upon z by h and the segments into which it divides z by z_1 and z_2, z_1 being adjacent to x and z_2 adjacent to y, then we have

$$h^2=x^2-z_1^2=y^2-z_2^2, \quad z_1+z_2=z. \tag{1}$$

These equations must be satisfied if x, y, z are to be the sides of a rational triangle. Moreover, if they are satisfied by positive rational numbers x, y, z, z_1, z_2, h, then x, y, z, h are in order the sides and altitude upon z of a rational triangle. Hence the problem of determining all rational triangles is equivalent to that of finding all positive rational solutions of system (1).

From Eqs. (1) it follows readily that rational numbers m and n exist such that

$$x+z_1=m, \quad x-z_1=\frac{h^2}{m};$$

$$y+z_2=n, \quad y-z_2=\frac{h^2}{n}.$$

Hence x, y, and z, where $z=z_1+z_2$, have the form

$$x=\frac{1}{2}\left(m+\frac{h^2}{m}\right),$$

$$y=\frac{1}{2}\left(n+\frac{h^2}{n}\right),$$

$$z=\frac{1}{2}\left(m+n-\frac{h^2}{m}-\frac{h^2}{n}\right),$$

respectively. If we suppose that each side of the given triangle is multiplied by $2mn$ and that x, y, z are then used to denote the sides of the resulting triangle, we have

$$\left.\begin{aligned} x&=n(m^2+h^2),\\ y&=m(n^2+h^2),\\ z&=(m+n)(mn-h^2).\end{aligned}\right\} \tag{2}$$

It is obvious that the altitude upon the side z is now $2hmn$, so that the area of the triangle is

$$hmn(m+n)(mn-h^2). \tag{3}$$

From this argument we conclude that the sides of any rational triangle are proportional to the values of x, y, z in (2), the factor of proportionality being a rational number. If we call this factor ρ, then a triangle having the sides ρx, ρy, ρz, where x, y, z are defined in (2), has its area equal to ρ^2 times the number in (3). Hence we conclude as follows:

A necessary and sufficient condition that rational numbers x, y, z shall represent the sides of a rational triangle is that they shall be proportional to numbers of the form $n(m^2+h^2)$, $m(n^2+h^2)$, $(m+n)(mn-h^2)$, where m, n, h are positive rational numbers and $mn>h^2$.

Let d represent the greatest common denominator of the rational fractions m, n, h, and write

$$m=\frac{\mu}{d}, \quad n=\frac{\nu}{d}, \quad h=\frac{k}{d}.$$

If we multiply the resulting values of x, y, z in (2) by d^3 we are led to the integral triangle of sides $\bar{x}$, $\bar{y}$, $\bar{z}$, where

$$\bar{x}=\nu(\mu^2+k^2),$$
$$y=\mu(\nu^2+k^2),$$
$$\bar{z}=(\mu+\nu)(\mu\nu-k^2).$$

With a modified notation the result may be stated in the following form:

Every rational integral triangle has its sides proportional to numbers of the form $n(m^2+h^2)$, $m(n^2+h^2)$, $(m+n)(mn-h^2)$, *where* m, n, h *are positive integers and* $mn>h^2$.

To obtain a special example we may put $m=4$, $n=3$, $h=1$. Then the sides of the triangle are 51, 40, 77 and the area is 924.

For further properties of rational triangles the reader may consult an article by Lehmer in *Annals of Mathematics*, second series, Volume I, pp. 97–102.

EXERCISES

1. Obtain the general rational solution of the equation

$$(x+y+z)xyz=u^2.$$

SUGGESTION.—Recall the interpretation of this equation as given in § 2.

2. Show that the cosine of an angle of a rational triangle can be written in one of the forms

$$\frac{\alpha^2-\beta^2}{\alpha^2+\beta^2}, \quad \frac{2\alpha\beta}{\alpha^2+\beta^2},$$

where α and β are relatively prime positive integers.

3. If x, y, z are the sides of a rational triangle, show that positive numbers α and β exist such that one of the equations,

$$x^2-2xy\frac{\alpha^2-\beta^2}{\alpha^2+\beta^2}+y^2=z^2, \quad x^2-2xy\frac{2\alpha\beta}{\alpha^2+\beta^2}+y^2=z^2,$$

is satisfied. Thence determine general expressions for x, y, z.

§ 5. Impossibility of the System $x^2+y^2=z^2$, $y^2+z^2=t^2$. Applications

By means of the result at the close of § 3 we shall now prove the following theorem:

I. *There do not exist integers x, y, z, t, all different from zero, such that*

$$x^2+y^2=z^2, \quad y^2+z^2=t^2. \tag{1}$$

It is obvious that an equivalent theorem is the following:

II. *There do not exist integers x, y, z, t, all different from zero, such that*

$$t^2+x^2=2z^2, \quad t^2-x^2=2y^2. \tag{2}$$

It is obvious that there is no loss of generality if in the proof we take x, y, z, t to be positive; and this we do.

The method of proof is to assume the existence of integers satisfying (1) and (2) and to show that we are thus led to a contradiction. The argument we give is an illustration of Fermat's famous method of "infinite descent," of which we give a general account in the next section.

If any two of the numbers x, y, z, t have a common prime factor p, it follows at once from (1) and (2) that all four of them have this factor. For, consider an equation in (1) or in (2) in which the two numbers divisible by p occur; this equation contains a third number of the set x, y, z, t, and it is readily seen that this third number is divisible by p. Then from one of the equations containing the fourth number it follows that this fourth number is divisible by p. Now let us divide each equation of systems (1) and (2) by p^2; the resulting systems are of the same forms as (1) and (2) respectively. If any two numbers in these resulting systems have a common prime factor p_1, we may divide each system through by p_1^2; and so on. Hence if a pair of simultaneous equations (2) exists then there exists a pair of equations of the same form in which no two of the numbers x, y, z, t have a common factor other than unity. Let this system of equations be

$$t_1^2+x_1^2=2z_1^2, \quad t_1^2-x_1^2=2y_1^2. \tag{3}$$

From the first equation in (3) it follows that t_1 and x_1 are both odd or both even; and, since they are relatively prime, it follows that they are both odd. Evidently $t_1 > x_1$. Then we may write

$$t_1 = x_1 + 2\alpha,$$

where α is a positive integer. If we substitute this value of t_1 in the first equation in (3), the result may readily be put in the form

$$(x_1+\alpha)^2 + \alpha^2 = z_1^2. \tag{4}$$

Since x_1 and z_1 have no common prime factor it is easy to see from this equation that α is prime to both x_1 and z_1, and hence that no two of the numbers $x_1+\alpha$, α, z_1 have a common factor other than unity.

Then, from the general result at the close of § 3 it follows that relatively prime positive integers r and s exist, where $r > s$, such that

$$x_1+\alpha = 2rs, \qquad \alpha = r^2 - s^2, \tag{5}$$

or

$$x_1+\alpha = r^2 - s^2, \quad \alpha = 2rs. \tag{6}$$

In either case we have

$$t_1^2 - x_1^2 = (t_1 - x_1)(t_1 + x_1) = 2\alpha \cdot 2(x_1+\alpha) = 8rs(r^2-s^2).$$

If we substitute in the second equation of (3) and divide by 2, we have

$$4rs(r^2-s^2) = y_1^2.$$

From this equation and the fact that r and s are relatively prime, it follows at once that r, s, r^2-s^2 are all square numbers; say

$$r = u^2, \quad s = v^2, \quad r^2 - s^2 = w^2.$$

Now $r-s$ and $r+s$ can have no common factor other than 1 or 2; hence, from

$$w^2 = r^2 - s^2 = (r-s)(r+s) = (u^2-v^2)(u^2+v^2)$$

we see that either

$$u^2+v^2 = 2w_1^2, \quad u^2-v^2 = 2w_2^2, \tag{7}$$

or

$$u^2+v^2 = w_1^2, \quad u^2-v^2 = w_2^2.$$

And if it is the latter case which arises, then

$$w_1^2+w_2^2=2u^2, \quad w_1^2-w_2^2=2v^2. \tag{8}$$

Hence, assuming equations of the form (2), we are led either to Eqs. (7) or to Eqs. (8); that is, we are led to new equations of the form with which we started. Let us write the equations thus:

$$t_2^2+x_2^2=2z_2^2, \quad t_2^2-x_2^2=2y_2^2; \tag{9}$$

that is, system (9) is identical with that one of systems (7), (8) which actually arises.

Now from (5) and (6) and the relations $t_1=x_1+2\alpha$, $r>s$, we see that

$$t_1=2rs+r^2-s^2>2s^2+r^2-s^2=r^2+s^2=u^4+v^4.$$

Hence $u<t_1$. Also,

$$w_1^2\leqq w^2\leqq r+s<r^2+s^2.$$

Hence $w_1<t_1$. Since u and w_1 are both less than t_1, it follows that t_2 is less than t_1. Hence, obviously, $t_2<t$. Moreover, it is clear that all the numbers x_2, y_2, z_2, t_2 are different from zero.

From these results we have the following conclusion: If we assume a system of the form (2) for given values of x, y, z, t, we are led to a new system (9) of the same form; and in the new system t_2 is less than t.

Now if we start with (9) and carry out a similar argument we shall be led to a new system

$$t_3^2+x_3^2=2z_3^2, \quad t_3^2-x_3^2=2y_3^2,$$

with the relation $t_3<t_2$; starting from this last system we shall be led to a new one of the same form, with a similar relation of inequality; and so on *ad infinitum*. But, since there is only a finite number of integers less than the given positive integer t, this is impossible. We are thus led to a contradiction; whence we conclude at once to the truth of II and likewise of I.

By means of theorems I and II we may readily prove the following theorem:

III. *The area of a Pythagorean triangle is never equal to a square number.*

Let the legs and hypotenuse of a Pythagorean triangle be u, v, w, respectively. The area of this triangle is $\frac{1}{2}uv$. If we assume this to be a square number ρ^2, we shall have the following simultaneous Diophantine equations:

$$u^2+v^2=w^2, \quad uv=2\rho^2. \tag{10}$$

We shall prove our theorem by showing that the assumption of such a system for given values of u, v, w, ρ leads to a contradiction.

From system (10) it is easy to show that if any two of the numbers u, v, w have the common prime factor p, then the remaining one of these numbers and the number ρ are both divisible by p. Thence it is easy to show that if any system of the form (10) exists there exists one in which u, v, w are prime each to each. We shall now suppose that (10) itself is such a system.

Since u, v, w are relatively prime it follows from the first equation in (10) and the theorem in § 3 that relatively prime integers a and b exist such that u, v have the values $2ab$, a^2-b^2 in some order. Hence from the second equation in (10) we have

$$\rho^2=ab(a^2-b^2)=ab(a-b)(a+b).$$

It is easy to see that no two of the numbers a, b, $a-b$, $a+b$, have a common factor other than unity; for, if so, u and v would fail to satisfy the restriction of being relatively prime. Hence from the last equation it follows that each of these numbers is a square. That is, we have equations of the form

$$a=m^2, \quad b=n^2, \quad a+b=p^2, \quad a-b=q^2;$$

whence

$$m^2-n^2=q^2, \quad m^2+n^2=p^2.$$

But, according to theorem I, no such system of equations can exist. That is, the assumption of Eqs. (10) leads to a contradiction. Hence the theorem follows as stated above.

From the last theorem we have an almost immediate proof of the following:

IV. *There are no integers x, y, z, all different from zero, such that*

$$x^4 - y^4 = z^2. \tag{11}$$

If we assume an equation of the form (11), we have

$$(x^4 - y^4)x^2y^2 = x^2y^2z^2. \tag{12}$$

But, obviously,

$$(2x^2y^2)^2 + (x^4 - y^4)^2 = (x^4 + y^4)^2. \tag{13}$$

Now, from (12), we see that the Pythagorean triangle determined by (13) has its area $(x^4 - y^4)x^2y^2$ equal to the square number $x^2y^2z^2$. But this is impossible. Hence no equation of the form (11) exists.

COROLLARY. *There exist no integers x, y, z, all different from zero, such that*

$$x^4 + y^4 = z^4.$$

EXERCISES

1. The system $x^2 - y^2 = ku^2$, $x^2 + y^2 = kv^2$ is impossible in integers x, y, k, u, v, all of which are different from zero.

2. The equation $x^4 + 4y^4 = z^2$ is impossible in integers x, y, z, all of which are different from zero.

3. The equation $2x^4 + 2y^4 = z^2$ is impossible in integers x, y, z, except for the trivial solution $z = \pm 2x^2 = \pm 2y^2$.

§ 6. THE METHOD OF INFINITE DESCENT

In the preceding section we have had an example of Fermat's famous method of infinite descent. In its relation to Diophantine equations this method may be broadly characterized as follows:

Suppose that one desires to prove the impossibility of the Diophantine equation

$$f(x_1, x_2, \ldots, x_n) = 0, \tag{1}$$

where f is a given function of its arguments. One assumes that the given equation is true for given values of $x_1, x_2, \ldots, x_n$, and shows that this assumption leads to a contradiction in the following particular manner. One proves the existence

of a set of integers $u_1, u_2, \ldots, u_n$ and a function $g(u_1, u_2, \ldots, u_n)$ having only positive integral values such that

$$f(u_1, u_2, \ldots, u_n) = 0, \tag{2}$$

while

$$g(u_1, u_2, \ldots, u_n) < g(x_1, x_2, \ldots, x_n).$$

The same process may then be applied to Eq. (2) to prove the existence of a set of integers $v_1, v_2, \ldots, v_n$, such that

$$f(v_1, v_2, \ldots, v_n) = 0, \quad g(v_1, v_2, \ldots, v_n) < g(u_1, u_2, \ldots, u_n).$$

This process may evidently be repeated an indefinite number of times. Hence there must be an indefinite number of different positive integers less than $g(x_1, x_2, \ldots, x_n)$. But this is impossible. Hence the assumption of Eq. (1) for a given set of values $x_1, \ldots, x_n$ leads to a contradiction; and therefore (1) is an impossible equation.

By a natural extension the method may also be employed (but usually not so readily) to find all the solutions of certain possible equations. It is also applicable, in an interesting way, to the proof of a number of theorems; one of these is the theorem that every prime number of the form $4\mu + 1$ is a sum of two squares of integers. See lemma II of § 10.

We shall now apply this method to the proof of the following theorem:

I. *There are no integers x, y, z, all different from zero, satisfying either of the equations*

$$x^4 - 4y^4 = \pm z^2. \tag{3}$$

Let us assume the existence of one of the equations (3) for a given set of positive integers x, y, z. If any two of these numbers have a common odd prime factor p, then all three of them have this factor, and the equation may be divided through by p^4. The new equation thus obtained is of the same form as the original one. The process may be repeated until an equation

$$x_1^4 - 4y_1^4 = \pm z_1^2$$

is obtained, in which no two of the numbers x_1, y_1, z_1 have a common odd prime factor.

If z_1 is even, it is obvious that x_1 is also even, and therefore the above equation may be divided through by 4; a result of the form

$$y_2^4 - 4x_2^4 = \mp z_2^2$$

is obtained. The process may be continued until an equation of one of the forms

$$y_3^4 - 4x_3^4 = \pm z_3^2$$

is obtained, in which z_3 is an odd number. Then y_3 is also odd. Then if the second member in the last equation has the minus sign we may write $y_3^4 + z_3^2 = 4x_3^4$. This equation is impossible, since the sum of two odd squares is obviously divisible by 2 but not by 4. Hence we must have

$$4x_3^4 + z_3^2 = y_3^4. \tag{4}$$

Now it is clear that no two of the numbers x_3, y_3, z_3 have a common factor other than unity and that all of them are positive. Hence, from the last equation it follows (by means of the result in § 3) that relatively prime positive integers r and s, $r > s$, exist such that

$$x_3^2 = rs, \quad z_3 = r^2 - s^2, \quad y_3^2 = r^2 + s^2.$$

From the first of these equations it follows that r and s are squares; say $r = \rho^2$, $s = \sigma^2$. Then from the last exposed equation we have

$$\rho^4 + \sigma^4 = y_3^2.$$

It is easy to see that ρ, σ, y_3 are prime each to each.

The last equation leads to relations of the form

$$y_3 = r_1^2 + s_1^2, \quad \rho^2 = 2r_1 s_1, \qquad \sigma^2 = r_1^2 - s_1^2,$$

or of the form

$$y_3 = r_1^2 + s_1^2, \quad \rho^2 = r_1^2 - s_1^2, \quad \sigma^2 = 2r_1 s_1.$$

In either case we see that $2r_1 s_1$ and $r_1^2 - s_1^2$ are squares, while r_1 and s_1 are relatively prime and one of them is even. From the relation $r_1^2 - s_1^2 = \text{square}$, it follows that r_1 is odd, since otherwise we should have the sum of two odd squares equal to the even square r_1^2, which is impossible. Hence s_1 is even.

But $2r_1s_1 = \text{square}$. Hence positive integers ρ_1, σ_1, exist such that $r_1 = \rho_1^2$, $s_1 = 2\sigma_1^2$. Hence, we have an equation of the form $\rho_1^4 - 4\sigma_1^4 = w_1^2$, since $r_1^2 - s_1^2$ is a square; that is, we have

$$4\sigma_1^4 + w_1^2 = \rho_1^4. \tag{5}$$

Now the last equation has been obtained solely from Eq. (4). Moreover, it is obvious that all the numbers ρ_1, σ_1, w_1, are positive. Also, we have

$$x_3^2 = rs = \rho^2\sigma^2 = 2r_1s_1(r_1^2 - s_1^2) = 4\rho_1^2\sigma_1^2(\rho_1^4 - 4\sigma_1^4) = 4\rho_1^2\sigma_1^2w_1^2.$$

Hence, $\sigma_1 < x_3$. Similarly, starting from (5) we should be led to an equation

$$4\sigma_2^4 + w_2^2 = \rho_2^4,$$

where $\sigma_2 < \sigma_1$; and so on indefinitely. But such a recursion is impossible. Hence, the theorem follows as stated above.

By means of this result we may readily prove the following theorem:

II. *The area of a Pythagorean triangle is never equal to twice a square number.*

For, if there exists a set of rational numbers u, v, w, t such that

$$u^2 + v^2 = w^2, \quad uv = t^2,$$

then it is easy to see that

$$(u+v)^2 = w^2 + 2t^2, \quad (u-v)^2 = w^2 - 2t^2;$$

or,

$$w^4 - 4t^4 = (u^2 - v^2)^2.$$

Again, we have the following:

III. *There are no integers x, y, z, all different from zero, such that*

$$x^4 + y^4 = z^2.$$

For, if such an equation exists, we have a Pythagorean triangle $(x^2)^2 + (y^2)^2 = z^2$, whose area $\frac{1}{2}x^2y^2$ is twice a square number; but this is impossible.

EXERCISES

1. In a Pythagorean triangle $x^2+y^2=z^2$, prove that not more than one of the sides x, y, z, is a square number. (Cf. Exs. 4, 5, 6 in § 3.)

2. Show that the number expressing the area of a Pythagorean triangle has at least one odd prime factor entering into it to an odd power and thence show that every number of the form $\rho^4-\sigma^4$, in which ρ and σ are different positive integers, has always an odd prime factor entering into it to an odd power.

3. The equation $2x^4-2y^4=z^2$ is impossible in integers x, y, z, all of which are different from zero.

4. The equation $x^4+2y^4=z^2$ is impossible in integers x, y, z, all of which are different from zero.

Suggestion.—This may be proved by the method of infinite descent. (Euler's Algebra, 22, § 210.) Begin by writing z in the form

$$z=x^2+\frac{2py^2}{q},$$

where p and q are relatively prime integers, and thence show that $x^2=q^2-2p^2$, $y^2=2pq$, provided that x, y, z are prime each to each.

5. By inspection or otherwise obtain several solutions of each of the equations $x^4-2y^4=z^2$, $2x^4-y^4=z^2$, $x^4+8y^4=z^2$.

6. The equation $x^4-y^4=2z^2$ is impossible in integers x, y, z, all of which are different from zero.

7. The equation $x^4+y^4=2z^2$ is impossible in integers x, y, z, except for the trivial solution $z=\pm x^2=\pm y^2$.

8. The equation $8x^4-y^4=z^2$ is impossible in integers x, y, z, all of which are different from zero.

9. The equation $x^4-8y^4=z^2$ is impossible in integers x, y, z, all of which are different from zero.

GENERAL EXERCISES

1. Find the general rational solution of the equation $x^2+y^2=a^2$, where a is a given rational number.

2. Find the general rational solution of the equation $x^2+y^2=a^2+b^2$, where a and b are given rational numbers.

3. Determine all primitive Pythagorean triangles of which the perimeter is a square.

4. Find general formulæ for the sides of a primitive Pythagorean triangle such that the sum of the hypotenuse and either leg is a cube.

5. Find general formulæ for the sides of a primitive Pythagorean triangle such that the hypotenuse shall differ from each side by a cube.

6. Observe that the equation $x^2+y^2=z^2$ has the three solutions

$$x=2mn, \quad y=m^2-n^2, \quad z=m^2+n^2,$$

where

$$m=k^2+kl+l^2, \quad n=k^2-l^2;$$

$$m=k^2+kl+l^2, \quad n=2kl+l^2;$$

$$m=k^2+2kl, \quad n=k^2+kl+l^2;$$

and show that each of the three Pythagorean triangles so determined has the area

$$(k^2+kl+l^2)(k^2-l^2)(2k+l)(2l+k)kl. \qquad \text{(Hillyer, 1902.)}$$

7.* Develop methods of finding an infinite number of positive integral solutions of the Diophantine system

$$x^2+y^2=u^2,\ y^2+z^2=v^2,\ z^2+x^2=w^2.$$

(See *Amer. Math. Monthly*, Vol. XXI, p. 165, and *Encyclopédie des sciences mathématiques*, Tome I, Vol. III, p. 31).

8.* Obtain intergal solutions of the Diophantine system.

$$x^2+y^2=t^2=z^2+w^2,\ x^2-w^2=u^2=z^2-y^2.$$

9. Solve the Diophantine system $x^2+t=u^2,\ x^2-t=v^2$.

10. Find three squares in arithmetical progression.

CHAPTER II

PROBLEMS INVOLVING A MULTIPLICATIVE DOMAIN

§ 7. On Numbers of the Form $x^2+axy+by^2$

Numbers of the form m^2+n^2 have a remarkable property which is closely connected with the fact that the equation $x^2+y^2=z^2$ has a simple and elegant theory. This property is expressed by means of the identities

$$\begin{aligned}(m^2+n^2)(p^2+q^2) &= (mp+nq)^2+(mq-np)^2,\\ &= (mp-nq)^2+(mq+np)^2. \qquad (1)\end{aligned}$$

A part of what is contained in these relations may be expressed in words as follows: the product of two numbers of the form m^2+n^2 is itself of the same form and in general in two ways.

If in (1) we put $p=m$ and $q=n$, we have

$$(m^2-n^2)^2+(2mn)^2=(m^2+n^2)^2.$$

Thus we are led to the fundamental solution

$$x=m^2-n^2, \quad y=2mn, \quad z=m^2+n^2,$$

of the Pythagorean equation $x^2+y^2=z^2$.

In a similar manner, from the relations

$$\begin{aligned}(m^2+n^2)^3=(m^2+n^2)^2(m^2+n^2) &= [(m^2-n^2)^2+(2mn)^2](m^2+n^2)\\ &= (m^3+mn^2)^2+(m^2n+n^3)^2,\\ &= (m^3-3mn^2)^2+(3m^2n-n^3)^2,\end{aligned}$$

we have for the equation $x^2+y^2=z^3$ the following two double parameter solutions

$$\begin{aligned}x&=m^3+mn^2, \quad y= m^2n+n^3, \quad z=m^2+n^2;\\ x&=m^3-3mn^2, \quad y=3m^2n-n^3, \quad z=m^2+n^2.\end{aligned}$$

Thus, if we take $m=2$, $n=1$, we have $10^2+5^2=5^3$, and $2^2+11^2=5^3$.

It is obvious that we may in a similar way obtain two-parameter solutions of the equation $x^2+y^2=z^k$ for every positive integral value of k.

Again from (1) we see that the equation

$$x^2+y^2=u^2+v^2$$

has the four-parameter solution

$$x=mp+nq, \quad y=mq-np, \quad u=mp-nq, \quad v=mq+np.$$

Thus, if we put $m=3$, $n=2$, $p=2$, $q=1$, we have in particular $8^2+1^2=4^2+7^2$.

There are several kinds of forms which have the same remarkable property as that pointed out above for the form m^2+n^2. Thus we have, in particular,

$$(m^2+amn+bn^2)(p^2+apq+bq^2)=r^2+ars+bs^2, \qquad (2)$$

when

$$r=mp-bnq, \quad s=np+mq+anq,$$

as one may readily verify by actual multiplication. This is a special case of a general formula which will be developed in § 12 in such a way as to throw light on the reason for its existence. A special case of it will be treated in detail in § 8.

EXERCISES

1. Find a two-parameter solution of the equation $x^2+axy+by^2=z^2$.

2. Find a two-parameter solution of the equation $x^2+axy+by^2=z^3$.

3. Describe a method for finding two-parameter solutions of the equation $x^2+axy+by^2=z^k$ for any given positive integral value of k.

4. Show that $(m^2+amn+n^2)(p^2+apq+q^2)=r^2+ars+s^2$, where r, s have either of the two sets of values

$$r=mp-nq, \quad s=np+mq+anq;$$

$$r=mq-np, \quad s=nq+mp+anp.$$

5. Find a four-parameter solution of the equation

$$x^2+axy+y^2=u^2+auv+v^2.$$

6. Find a six-parameter solution of the system

$$x^2+axy+y^2=u^2+auv+v^2=z^2+azt+t^2.$$

7. Find a two-parameter integral solution of the equation $x^2+y^2=z^2+1$.

§ 8. On the Equation $x^2 - Dy^2 = z^2$

We shall now develop a general theory by means of which the solutions of the equation

$$x^2 - Dy^2 = z^2 \tag{1}$$

may be found. Naturally D is assumed to be an integer. Without loss of generality it may be taken positive; for if it were negative the equation might be written in the form $z^2 - (-D)y^2 = x^2$, where $-D$ is positive. If D is the square of an integer, say, $D = d^2$, the equation may be written

$$x^2 = z^2 + (dy)^2,$$

so that the theory becomes essentially that of the Pythagorean equation $x^2 + y^2 = z^2$. Accordingly, we shall suppose that D is not a square.

By suitably specializing Eq. (2) of the preceding section we readily obtain the following two-parameter solution of (1):

$$x = m^2 + Dn^2, \quad y = 2mn, \quad z = m^2 - Dn^2.$$

But there is no ready means for determining whether this is the general solution. Consequently we shall approach from another direction the problem of finding the solution of (1).

We shall first show that Eq. (1) possesses a non-trivial solution for which $z = 1$; that is, we shall prove the existence of a solution of the equation

$$x^2 - Dy^2 = 1. \tag{2}$$

different from the trivial solutions $x = \pm 1$, $y = 0$.

For this purpose we shall first show that *integers u, v exist such that the absolute value* * *of the (positive or negative) real quantity $u - v\sqrt{D}$ is less than $1/v$ and also less than any pre-assigned positive constant ϵ.* (By $\sqrt{D}$ we mean the positive square root of D.) Let t be an integer such that $t\epsilon > 1$. Now give to v successively the integral values from 0 to t and in each case choose for u the least integral value greater than

* By the absolute value of A is meant A itself when A is positive and $-A$ when A is negative. We denote it by $|A|$.

$v\sqrt{D}$. In each case the quantity $u-v\sqrt{D}$ lies between 0 and 1 and in no two cases are its values equal. If we divide the interval from 0 to 1 into t subintervals, each of length $1/t$, then two of the above values of $u-v\sqrt{D}$, say $u'-v'\sqrt{D}$ and $u''-v''\sqrt{D}$, must lie in the same interval. Then the expression

$$(u'-u'')-(v'-v'')\sqrt{D}$$

is different from zero, is of the form $u-v\sqrt{D}$ and has an absolute value less than $1/t$ and hence less than ϵ. That this absolute value is less than that of $1/(v'-v'')$ follows from the fact that the difference of v' and v'' is not greater than t. This completes the proof of the above statement concerning the existence of u, v with the assigned properties.

From the existence of one such set of integers u, v it follows readily that there is an infinite number of such sets. For, let u, v be one such set. Let ϵ_1 be a positive constant less than $|u-v\sqrt{D}|$. Then integers u_1, v_1 can be determined such that $u_1-v_1\sqrt{D}$ is in absolute value less than $1/v_1$, and also less than ϵ_1. It is then less than ϵ. Thus we have a second set u_1, v_1 satisfying the original conditions. Then, letting ϵ_2 be a positive constant less than $|u_1-v_1\sqrt{D}|$, we may proceed as before to find a third set u_2, v_2 with the required properties. It is obvious that this process may be continued indefinitely and that we are thus led to an infinite number of sets of integers u, v such that $u-v\sqrt{D}$ is in absolute value less than ϵ and also less than the absolute value of $1/v$.

Now let u and v be a pair of integers determined as above. Then we have

$$|u+v\sqrt{D}| \leqq |u-v\sqrt{D}|+|2v\sqrt{D}| < \left|\frac{1}{v}\right|+|2v\sqrt{D}|.$$

Hence

$$|u^2-Dv^2| = |u+v\sqrt{D}|\cdot|u-v\sqrt{D}| < \left|\frac{1}{v}\right|\left\{\left|\frac{1}{v}\right|+|2v\sqrt{D}|\right\},$$

so that

$$|u^2-Dv^2| < \frac{1}{v^2}+2\sqrt{D} < 1+2\sqrt{D}.$$

Since $|u^2-Dv^2|$ is less than $1+2\sqrt{D}$ for every one of the infinite number of sets u, v in consideration, and since its value

is always integral, it follows that an integer l exists such that

$$u^2 - Dv^2 = l$$

for an infinite number of sets of values u, v. It is then obvious that there is an infinite number of these pairs u_1, v_1; u_2, v_2; u_3, v_3; . . ., such that $u_i - u_j$ and $v_i - v_j$ are both divisible by l for every i and j. Let u', v'; u'', v'' be two pairs belonging to this last infinite subset and chosen so that $u'' \neq \pm u'$ and $v'' \neq \pm v'$. It is obvious that this choice is possible. From the equations

$$u'^2 - Dv'^2 = l, \quad u''^2 - Dv''^2 = l,$$

we have (by Formula (2) of § 7):

$$(u'u'' - Dv'v'')^2 - D(u'v'' - u''v')^2 = l^2.$$

Here we take $u' = m$, $u'' = p$, $v' = n$, $v'' = -q$, $D = -b$, in applying the formula referred to.

Setting

$$x = \frac{u'u'' - Dv'v''}{l}, \quad y = \frac{u'v'' - u''v'}{l}, \tag{3}$$

we have

$$x^2 - Dy^2 = 1. \tag{4}$$

It remains to show that the values of x and y in (3) are integers. On account of (4) it is obviously sufficient to show that y is an integer. That y is an integer follows at once from the equations $u' = u'' + \mu l$, $v'' = v' + \nu l$, by multiplication member by member. We show further that $y \neq 0$. If we suppose that $y = 0$, we have

$$u'v'' - u''v' = 0, \quad u'u'' - Dv'v'' = \pm l.$$

These equations are satisfied only if $u'' = \pm u'$, $v'' = \pm v'$, relations which are contrary to the hypothesis concerning u', u'', v', v''.

We have thus established the fact that Eq. (2) has at least one integral solution which is not trivial. Since we may associate with any solution x, y of (2) the other solutions $-x$, y; $-x$, $-y$; x, $-y$; it is clear that there is at least one solution of (2) in which x and y are positive.

Let x_1, y_1, and x_2, y_2 be any solutions of (2), whether the same or different. Then we have

$$1 = (x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2) = (x_1x_2 + Dy_1y_2)^2 - D(x_1y_2 + x_2y_1)^2,$$

so that $x_1x_2 + Dy_1y_2$ and $x_1y_2 + x_2y_1$ afford a solution of (2). Hence from the solution x, y, whose existence has already been proved, we have a second solution $x^2 + Dy^2$, $2xy$. It is easy to show that this process may be continued and that it will lead to an infinite number of solutions of (2). But this problem is a special case of one to be treated presently; and hence will not be further pursued now.

In order to come upon the more general problem let us seek solutions of Eq. (1) in which z shall have the positive value σ; that is, let us seek solutions of the equation

$$x^2 - Dy^2 = \sigma^2. \tag{5}$$

If $x = x_1$, $y = y_1$ is a positive solution of Eq. (2) then it is clear that $x = \sigma x_1$, $y = \sigma y_1$ is a positive solution of (5). Hence from what precedes we have at least two positive solutions of (5).

Now let $x = t_1$, $y = u_1$; $x = t_2$, $y = u_2$ be any two solutions of Eq. (5) and write

$$\frac{t_1 + u_1\sqrt{D}}{\sigma} \cdot \frac{t_2 + u_2\sqrt{D}}{\sigma} = \frac{t + u\sqrt{D}}{\sigma}, \tag{6}$$

where t and u are rational numbers. Then

$$\left.\begin{aligned} t &= \frac{t_1t_2 + Du_1u_2}{\sigma}, \\ u &= \frac{t_1u_2 + t_2u_1}{\sigma}. \end{aligned}\right\} \tag{7}$$

From (6) we have

$$\frac{t_1 - u_1\sqrt{D}}{\sigma} \cdot \frac{t_2 - u_2\sqrt{D}}{\sigma} = \frac{t - u\sqrt{D}}{\sigma}. \tag{8}$$

Multiplying Eqs. (6) and (8) member by member and making use of the relations

$$t_1^2 - Du_1^2 = \sigma^2, \quad t_2^2 - Du_2^2 = \sigma^2, \tag{9}$$

we have

$$t^2 - Du^2 = \sigma^2. \tag{10}$$

Hence $x=t$, $y=u$ afford a rational solution of (5), t and u having the values given in (7).

We shall now point out two cases in which this solution is integral.

Suppose that σ^2 is a factor of D. Then from (9) it follows that σ is a factor of both t_1 and t_2 and hence from (7) that u is an integer. Then from (10) it follows that t is an integer.

Suppose that *

$$4D \equiv \sigma^2 \bmod 4\sigma^2;$$

that is, that σ^2 is a remainder obtained on dividing $4D$ by $4\sigma^2$. Then σ is evidently an even number. Write $\sigma=2\rho$. Then we have $D\equiv\rho^2 \bmod 4\rho^2$. Hence D is divisible by ρ^2. Then from (9) it follows that both t_1 and t_2 are divisible by ρ, since $\sigma=2\rho$. Put

$$D=d\rho^2, \quad t_1=\theta_1\rho, \quad t_2=\theta_2\rho.$$

Then d is odd. Moreover, the following relations exist, as we see from (9) and (7):

$$\theta_1^2-du_1^2=4, \quad \theta_2^2-du_2^2=4; \tag{11}$$

$$u=\tfrac{1}{2}(\theta_1u_2+\theta_2u_1). \tag{12}$$

From Eqs. (11) we see that θ_1 and u_1 are both odd or both even, and also that θ_2 and u_2 are both odd or both even. Then from (12) it follows that u is an integer and hence from (10) that t is an integer.

We are now in position to prove readily the following theorem:

Let D be any positive non-square integer and let σ be any positive integer such that $D\equiv 0 \bmod \sigma^2$ or $4D\equiv\sigma^2 \bmod 4\sigma^2$. Let $x=t_1$ and $y=u_1$ be the least positive integral solution of the equation

$$x^2-Dy^2=\sigma^2. \tag{5 bis}$$

Then all the positive integral solutions † of this equation are contained in the set

$$x=t_n, \quad y=u_n, \quad n=1, 2, 3, \ldots,$$

* The symbol $\equiv$ is read *is congruent to*. For the elementary properties of congruences see the author's *Theory of Numbers*, pp. 37–41.

† It is obvious that all integral solutions are readily obtainable from all positive integral solutions.

where

$$t_n=\frac{1}{\sigma^{n-1}}\left[t_1^n+\frac{n(n-1)}{2!}Dt_1^{n-2}u_1^2 + \frac{n(n-1)(n-2)(n-3)}{4!}D^2t_1^{n-4}u_1^4+\ldots\right],$$

$$u_n=\frac{1}{\sigma^{n-1}}\left[\frac{n}{1!}t_1^{n-1}u_1+\frac{n(n-1)(n-2)}{3!}Dt_1^{n-3}u_1^3+\ldots\right].$$

That all these values indeed afford solutions follows readily from the fact that the quantities t_n and u_n so defined satisfy the relation

$$\left(\frac{t_1+u_1\sqrt{D}}{\sigma}\right)^n=\frac{t_n+u_n\sqrt{D}}{\sigma}. \tag{13}$$

For then we also have

$$\left(\frac{t_1-u_1\sqrt{D}}{\sigma}\right)^n=\frac{t_n-u_n\sqrt{D}}{\sigma};$$

whence

$$t_n^2-Du_n^2=\sigma^2,$$

as one easily shows by multiplying the preceding two equations member by member and simplifying the result by means of the relation $t_1^2-Du_1^2=\sigma^2$. That these solutions are positive is obvious. That they are integral follows from the results associated with Eqs. (7) and (10).

It remains to be shown that there are no other positive integral solutions than those defined in the above theorem. Let $x=T$, $y=U$ be any positive integral solution of Eq. (5^{bis}). Then, from the relation

$$\frac{T+U\sqrt{D}}{\sigma}\cdot\frac{T-U\sqrt{D}}{\sigma}=\frac{T^2-DU^2}{\sigma^2}=1$$

it follows readily that

$$0<\frac{T-U\sqrt{D}}{\sigma}<1<\frac{T+U\sqrt{D}}{\sigma}.$$

Hence from (13) it follows that

$$\frac{t_n+u_n\sqrt{D}}{\sigma}<\frac{t_{n+1}+u_{n+1}\sqrt{D}}{\sigma}.$$

Now suppose that the solution T, U does not coincide with any solution given in the above theorem. Then for some value of n we have the relations:

$$\frac{t_n+u_n\sqrt{D}}{\sigma}<\frac{T+U\sqrt{D}}{\sigma}<\frac{t_{n+1}+u_{n+1}\sqrt{D}}{\sigma},$$

whence

$$\frac{t_n+u_n\sqrt{D}}{\sigma}<\frac{T+U\sqrt{D}}{\sigma}<\frac{t_n+u_n\sqrt{D}}{\sigma}\cdot\frac{t_1+u_1\sqrt{D}}{\sigma},$$

or

$$1<\frac{T+U\sqrt{D}}{\sigma}\cdot\frac{\sigma}{t_n+u_n\sqrt{D}}<\frac{t_1+u_1\sqrt{D}}{\sigma}.$$

But

$$\frac{\sigma}{t_n+u_n\sqrt{D}}=\frac{\sigma(t_n-u_n\sqrt{D})}{t_n^2-Du_n^2}=\frac{t_n-u_n\sqrt{D}}{\sigma}.$$

Thence we have

$$1<\frac{T+U\sqrt{D}}{\sigma}\cdot\frac{t_n-u_n\sqrt{D}}{\sigma}<\frac{t_1+u_1\sqrt{D}}{\sigma}.$$

Writing

$$\frac{T+U\sqrt{D}}{\sigma}\cdot\frac{t_n-u_n\sqrt{D}}{\sigma}=\frac{T'+U'\sqrt{D}}{\sigma},$$

where T' and U' are rational, we have $x=T'$, $y=U'$ as a solution of (5^{bis}). It is integral, as we see from the results associated with Eqs. (7) and (10). Moreover, the relations

$$1<\frac{T'+U'\sqrt{D}}{\sigma}<\frac{t_1+u_1\sqrt{D}}{\sigma} \tag{14}$$

are verified.

Since $(T'+U'\sqrt{D})(T'-U'\sqrt{D})=\sigma^2$, it follows from the first inequality in (14) that $T'-U'\sqrt{D}$ is positive and less than σ, and hence that T' and U' are both positive. If we suppose that $T'\geq t_1$, it follows from the relations, $T'^2-DU'^2=\sigma^2$, $t_1^2-Du_1^2=\sigma^2$, that $U'\geq u_1$, a result in contradiction with relation (14). Hence, $T'<t_1$ and $U'<u_1$. But this is contrary to the hypothesis that t_1, u_1 is the least positive integral solution of (5^{bis}). Hence the given positive solution T, U must coincide with one of those given in the theorem.

This completes the demonstration of the theorem.

It is clear that the value $\sigma = 1$ satisfies the requisite conditions on σ for every non-square integer D, so that the above theorem is applicable in particular to every equation of the form $x^2 - Dy^2 = 1$. In order to apply the theorem in a particular case it is necessary first to find, by inspection or otherwise,* the least positive integral solution.

As an illustrative example, let us consider the equation $x^2 - 7y^2 = 1$. If we try successively the values 1, 2, 3, . . . for y we find that 3 is the least positive integral value of y for which there is a corresponding integer x satisfying the given equation. This value is $x = 8$ so that $x = 8$, $y = 3$ is the least positive integral solution of the equation $x^2 - 7y^2 = 1$. Setting $D = 7$, $\sigma = 1$, $t_1 = 8$, $u_1 = 3$, in the last two equations of the above theorem, we have formulæ for the general positive integral solution of the equation $x^2 - 7y^2 = 1$. Giving n successively the values 1, 2, 3, . . ., the particular positive integral solutions are obtained without repetition and in the order of increasing magnitude. The first three of these solutions are

$$8, 3; \quad 127, 48; \quad 2024, 765.$$

EXERCISES

1. Show how all integral solutions of the equation $x^2 - Dy^2 = -1$ may be obtained from one of them, D being as usual a positive non-square integer.

SUGGESTION.—Observe that the relations $a^2 - Db^2 = -1$, $c^2 - Dg^2 = -1$ imply the relation $(ac + Dbg)^2 - D(ag + bc)^2 = 1$.

2. Solve each of the Diophantine equations $x^2 + 1 = 2y^2$, $x^2 - 1 = 2y^2$.

3. Let s_n represent the sum of the legs and h_n the hypotenuse of an integral Pythagorean triangle in which the legs differ by unity. Show that every possible pair of values s_n and h_n is determined by the relation

$$(1 + \sqrt{2})(3 + 2\sqrt{2})^n = s_n + h_n\sqrt{2},$$

s_n and h_n being rational.

4. Find all integral Pythagorean triangles in which the legs differ by 2.

5. Obtain the general integral solution of each of the equations $x^2 - 5y^2 = 4$, $x^2 - 20y^2 = 4$.

6. Obtain a formula giving an infinite number of integral solutions of the equation $x^2 - 19y^2 = 81$.

* How this may be done, by developing the numerical value of $\sqrt{D}$ into a continued fraction, is explained by Whitford, in *The Pell Equation* (New York, 1912). When D is 1620, the value of x has three figures; when D is 1621, it has 76 figures.

7. Find the general rational solution of the equation $x^2-Dy^2=4$. By means of this rational solution obtain an infinite number of integral solutions.

8. Find the smallest integral solutions of $x^2-1620y^2=1$ and $x^2-1666y^2=1$.

§ 9. General Equation of the Second Degree in Two Variables

Let us consider the general Diophantine equation of the second degree in two variables

$$ax^2+2bxy+cy^2+2dx+2ey+f=0, \tag{1}$$

where a, b, c, d, e, f are integers.

In case $ac-b^2=0$, the equation may be written in the form

$$(ax+by)^2+2adx+2aey+af=0.$$

In order to obtain rational solutions it is sufficient to put

$$ax+by=t, \quad 2adx+2aey+af=-t^2, \tag{2}$$

where t is any rational number, and solve these equations for x and y. This gives, in general,

$$\left.\begin{aligned} x&=\frac{-bt^2-2aet-abf}{2a(bd-ae)},\\ y&=\frac{t^2+2dt+af}{2(bd-ae)}. \end{aligned}\right\} \tag{3}$$

If the solution is to be integral, then t must be integral, as one sees from the first equation in (2). Then from (3) it follows that a necessary and sufficient condition on the integer t is that it shall satisfy the following congruences:

$$t^2+2dt+af\equiv 0 \bmod 2(bd-ae),$$

$$bt^2+2aet+abf\equiv 0 \bmod 2a(bd-ae).$$

In any particular case the general solution of this system of congruences may be determined by inspection.

In case $ac-b^2\neq 0$ the solution is not so easily determined. Multiplying Eq. (1) through by $(ac-b^2)^2$ we have a result which may be put in the form

$$au^2+2buv+cv^2=m, \tag{4}$$

where

$$\left.\begin{aligned} u &= (ac-b^2)x-(be-cd),\\ v &= (ac-b^2)y-(bd-ae),\\ m &= (ac-b^2)(ae^2+cd^2+fb^2-acf-2bde). \end{aligned}\right\} \qquad (5)$$

Thus the problem of solving Eq. (1) is reduced to that of solving Eq. (4) for u and v and choosing those values only of u and v for which x and y have the desired characteristic.* But the problem of solving Eq. (4) is identical with that of the representation of a given integer by means of a binary quadratic form. The plan of this book does not permit the detailed development of this latter subject. (See the preface.) Consequently the problem of solving Eq. (1) will be dismissed with this remark.

§ 10. Quadratic Equations Involving More than Three Variables

Having now developed the general theory of the equation

$$x^2+y^2=t^2,$$

and certain generalizations of it involving still a total of three variables, it is natural to extend the problem in another direction, namely, by increasing the number of variables. We should thus be led next to consider the equation

$$x^2+y^2+u^2=t^2. \qquad (1)$$

Now the classes of numbers which have been involved in the larger part of our previous theory and which have given rise to the most interesting results, namely, those defined by forms such as x^2+y^2 and x^2-Dy^2, have had the following remarkable property: the product of any two numbers in one of the classes is itself in that class. We shall express this fact by saying that the numbers of the class form a domain with respect to multiplication. The sets of numbers mentioned

* If an *integral* solution is desired we may choose those values only of u and v for which x and y are integral. When x and y are restricted merely to be *rational* every solution of (4) leads through (5) to a solution of (1).

also have this further property: from the representation of two numbers in the given form that of their product is readily obtained by means of an algebraic formula.

Numbers of the form $x^2+y^2+u^2$ do not form a domain with respect to multiplication. This may be shown by means of an example. We have

$$3=1^2+1^2+1^2, \quad 5=2^2+1^2+0^2, \quad 21=4^2+2^2+1^2,$$

while neither 15 nor 63 can be expressed as a sum of three integral squares.

But if we should enlarge the set of numbers $x^2+y^2+u^2$ so that the new set shall contain all numbers of the form $x^2+y^2+u^2+v^2$ then the set so enlarged forms a domain with respect to multiplication. This is a special case of a more general result which we shall presently give. In view of the existence of this domain with respect to multiplication we have a direct means of treating the problem of solving the equation

$$x^2+y^2+u^2+v^2=t^2. \tag{2}$$

Putting to zero the quantity representing v in this solution and restricting the values of x, y, u, t accordingly, we should arrive at a solution of Eq. (1).

We proceed at once to a more general problem including that concerning Eq. (1). Let us consider the Diophantine equation

$$x^2+ay^2+bu^2=t^2. \tag{3}$$

where a and b are given integers. When $a=b=1$ the equation is the same as (1). We shall first treat the more general equation

$$x^2+ay^2+bu^2+abv^2=t^2, \tag{4}$$

because, as we shall now show, the form of the first member defines a class of numbers which form a domain with respect to multiplication.

Let us employ the notation

$$g(x, y, u, v)=x^2+ay^2+bu^2+abv^2.$$

Then it may be readily verified that *

$$g(x, y, u, v) \cdot g(x_1, y_1, u_1, v_1) = g(x_2, y_2, u_2, v_2), \tag{5}$$

where

$$\left.\begin{aligned} x_2 &= xx_1 - ayy_1 - buu_1 + abvv_1, \\ y_2 &= xy_1 + x_1y - buv_1 - bu_1v, \\ u_2 &= ux_1 + u_1x + avy_1 + av_1y, \\ v_2 &= vx_1 - v_1x - uy_1 + u_1y. \end{aligned}\right\} \tag{6}$$

It is obvious that Eq. (5) will also be satisfied by values x_2, y_2, u_2, v_2 obtained from (6) by replacing any number of the quantities x, y, u, v, x_1, y_1, u_1, v_1 by their negatives. In case $a = b = 1$ still other values of x_2, y_2, u_2, v_2 may be obtained by any interchange of the quantities x, y, u, v or of the quantities x_1, y_1, u_1, v_1 among themselves. In case $a = 1$ and $b \neq 1$ the elements of the following pairs may be similarly interchanged: x, y; u, v; x_1, y_1; u_1, v_1. Not all the resulting values of x_2, y_2, u_2, v_2 will be distinct, though there will in general be two or more independent sets.

Thus we see that the class of numbers defined by the form $x^2 + ay^2 + bu^2 + abv^2$ form a domain with respect to multiplication and that the product of any two numbers of the class is readily expressible in the given form, and frequently in several ways.

From Eqs. (5) and (6) and the transformations of them indicated above, we have the following relations:

$$\left.\begin{aligned} \{g(x, y, u, v)\}^2 &= g(x^2 - ay^2 - bu^2 + abv^2,\ 2xy - 2buv,\ 2ux + 2avy,\ 0) \\ &= g(x^2 - ay^2 + bu^2 - abv^2,\ 2xy + 2buv,\ 0,\ 2vx - 2uy), \\ &= g(x^2 + ay^2 - bu^2 - abv^2,\ 0,\ 2ux - 2avy,\ 2vx + 2uy), \\ &= g(x^2 - ay^2 + bu^2 + abv^2,\ 2xy,\ 2avy,\ 2uy), \\ &= g(x^2 + ay^2 - bu^2 + abv^2,\ 2buv,\ 2ux,\ 2uy), \\ &= g(x^2 + ay^2 + bu^2 - abv^2,\ 2buv,\ 2avy,\ 2vx), \\ &= g(x^2 - ay^2 - bu^2 - abv^2,\ 2xy,\ 2ux,\ 2vx). \end{aligned}\right\} \tag{7}$$

* If in these relations we take $a = b = 1$ we shall have a set of formulæ to which one is led directly by means of quaternions. Thus if we write

$$(x + iy + ju - kv)(x_1 + iy_1 + ju_1 + kv_1) = x_2 + iy_2 + ju_2 + kv_2,$$

where i, j, k are the quaternion units, we may readily determine x_2, y_2, u_2, v_2, by direct multiplication of the quaternions in the first member. We obtain the values gotten from (6) by putting $a = b = 1$. Taking the norm of each member of the equation in this footnote we have the special case of equation (5) for which $a = b = 1$.

Let us return to the consideration of Eq. (4), writing it now in the form

$$\alpha^2+a\beta^2+b\rho^2+ab\sigma^2=t^2, \tag{8}$$

where α, β, ρ, σ, t are the integers to be determined. It is clear that we have a four parameter solution of this equation by taking $g(x, y, u, v)$ for the value of t and the arguments (in order) in any right member of (7) for the values of α, β, ρ, σ, respectively.

Similarly for the equation

$$\alpha^2+a\beta^2+b\rho^2=t^2, \tag{9}$$

we have the following four parameter solution:

$$\begin{aligned} t&=x^2+ay^2+bu^2+abv^2,\\ \alpha&=x^2-ay^2-bu^2+abv^2,\\ \beta&=2xy-2buv,\\ \rho&=2ux+2avy, \end{aligned}$$

where x, y, u, v are arbitrary integers. It is also possible to obtain three parameter solutions of (9) in several ways. For instance, by taking $x=v$ in next to the last equation in (7), we have the following solution:

$$t=ay^2+bu^2+abv^2,\quad \alpha=-ay^2+bu^2-abv^2,\quad \beta=2buv,\quad \rho=2avy.$$

Whether the above formulæ give the general integral solutions of Eqs. (8) and (9) for a given a and b when x, y, u, v are restricted to be integers is a question which is not answered in the preceding discussion. It appears to be difficult of treatment so long as a and b are unrestricted. We shall take it up only for the most interesting special case, namely, that of the equation

$$x^2+y^2+z^2=t^2, \tag{10}$$

This is a special case of Eq. (9). Modifying our notation, we may write the first solution obtained above in the form

$$\left.\begin{aligned} t&=m^2+n^2+p^2+q^2,\\ x&=m^2-n^2-p^2+q^2,\\ y&=2mn-2pq,\\ z&=2mp+2nq. \end{aligned}\right\} \tag{11}$$

For the case of Eq. (10) the other solutions obtained for Eq. (9) are special cases of that given in (11).

Taking $m=3$, $n=3$, $p=1$, $q=2$, we have the particular instance $3^2+14^2+18^2=23^2$.

We shall prove that formulæ (11) afford the general integral solution of Eq. (10) if each of the second members is multiplied by the arbitrary integral factor d. In this demonstration we shall have use for certain lemmas. These will first be proved. They constitute in themselves remarkable theorems. They are due to Fermat.

LEMMA I. *If a number is expressible as a sum of two integral squares $\alpha^2+\beta^2$ and if the quotient $(\alpha^2+\beta^2)/(a^2+b^2)$ is an integer m, where a and b are integers and a^2+b^2 is a prime number, then m is also a sum of two integral squares.*

We have

$$m=\frac{\alpha^2+\beta^2}{a^2+b^2}=\frac{(\alpha^2+\beta^2)(a^2+b^2)}{(a^2+b^2)^2}=\frac{(\alpha a+\beta b)^2+(\alpha b\mp\beta a)^2}{(a^2+b^2)^2}$$

$$=\left(\frac{\alpha a\pm\beta b}{a^2+b^2}\right)^2+\left(\frac{\alpha b\mp\beta a}{a^2+b^2}\right)^2.$$

It is sufficient to show that one of the numbers $\alpha a+\beta b$ is a multiple of a^2+b^2, and hence that their product is such a multiple, since a^2+b^2 is a prime. But their product is

$$\alpha^2a^2-\beta^2b^2=a^2(\alpha^2+\beta^2)-\beta^2(a^2+b^2)=(ma^2-\beta^2)(a^2+b^2).$$

Hence lemma I is established.

LEMMA II. *Every prime number of the form $4n+1$ can be represented in one and in only one way as a sum of two integral squares.*

We start from the theorem that -1 is a quadratic residue of every prime number of the form $4n+1$ and a quadratic non-residue of every prime number of the form $4n+3$. (See the author's *Theory of Numbers*, p. 70.) This is equivalent to saying that every prime number of the form $4n+1$ is a factor of a number of the form t^2+1 where t is a positive integer, while no prime number of the form $4n+3$ is a factor of such a number t^2+1. If we take for t the least integer such that

a prime number p of the form $4n+1$ is a factor of $P+1$, it is clear that we have the following relations:

$$P+1 = pk, \quad k < p.$$

Now consider the set of numbers

$$1^2+1,\ 2^2+1,\ 3^2+1,\ 4^2+1,\ \ldots\ldots \tag{12}$$

It is obvious that no one of these numbers contains two prime factors neither of which is a factor of a preceding number of the set, for if so the product of these primes must be a factor of a number $P+1$ with a complementary factor less than itself and hence less than the other prime.

Arrange all prime numbers not of the form $4n+1$ in the order in which they occur as factors of numbers in the set (12), thus

$$p_1 = 2,\ p_2 = 3,\ p_3 = 7,\ p_4 = 11,\ p_5 = 19,\ \ldots\ldots \tag{13}$$

The set contains every prime of the form $4n+1$.

Suppose that p_m is a prime number of the set (13) which is not expressible as a sum of two integral squares. Let $P+1$ be the first number of the set (12) of which p_m is a factor and by means of which p_m was assigned its place in (13). Then we have

$$p_m k_m = P+1 \tag{14}$$

where k_m is such that every prime factor of k_m appears earlier than p_m in the set (13). If every prime factor of k_m is a sum of two integral squares, then a repeated use of Lemma I in connection with Eq. (14) would lead to the conclusion that p_m is a sum of two integral squares. But this is contrary to the hypothesis concerning p_m. Hence there is some prime factor of k_m which is not expressible as a sum of two integral squares.

Thus we have proved that if any prime of the set (13) is not expressible as a sum of two integral squares, then there is an earlier prime in the same set which likewise is not expressible as a sum of two integral squares. This is in evident contradiction with the fact that the first prime of this set are each expressible as a sum of two squares. Hence every prime

in set (13), and hence every prime of the form $4n+1$, is expressible as a sum of two integral squares.

It remains to show that no prime p can be represented in two ways as a sum of two integral squares. This we shall do by assuming an equation of the form

$$p = a^2 + b^2 = c^2 + d^2 \qquad (14)$$

where a and c are even and b and d are odd, and proving that $a^2 = c^2$, $b^2 = d^2$. From (13) we have

$$p^2 = (ac + bd)^2 + (ad - bc)^2 = (ac - bd)^2 + (ad + bc)^2$$

$$p(a^2 - c^2) = c^2(a^2 + b^2) - a^2(c^2 + d^2) = (ac + bd)(ac - bd)$$

From the last equation it follows that p is a factor of one of the numbers $ac + bd$, $ac - bd$. Now neither of the numbers $a \pm b$ or $c \pm d$ is equal to zero since both of these are odd. Therefore, now next to the last equation we see that $ad - bc$ and $ad + bc$ are both less than p in absolute value. But one of these is divisible by p and hence that one is equal to zero. Therefore $a^2 - c^2 = 0$. From this relation and (14) it follows at once that $a^2 = c^2$, $b^2 = d^2$.

This completes the proof of lemma II.

It is obvious that no power of the form $4n+1$ can be represented as a sum of two integral squares, for if so one square must be even and the other odd, and in this case their sum is of the form $4n+1$.

LEMMA III. *Let p be any prime number of the form $4n+1$ and write $p = a^2 + b^2$, where a and b are integers. Let m be any integer such that $pm = c^2 + d^2$, where c and d are integers. Then there exists a representation of m as a sum of two integral squares,*

$$m = \left(\frac{ac + bd}{a^2 + b^2}\right)^2 + \left(\frac{ad \pm bc}{a^2 + b^2}\right)^2. \qquad (15)$$

and in the determination of $a^2 + b^2$ it can be obtained from the three representations of p and m by multiplication according to the formula

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

That m has the representation (16) was shown in the proof of lemma I. That this representation has the further property specified here may be verified by a direct computation.

COROLLARY. *If h is a composite number containing no prime factor of the form $4n+3$ and if we write $h=h_1h_2$, where h_1 and h_2 are positive integers, then every representation of h as a sum of two integral squares is obtained by taking every representation of h_1 and h_2 and multiplying these expressions in accordance with the formula*

$$(a^2+b^2)(c^2+d^2)=(ac\pm bd)^2+(ad\mp bc)^2.$$

We are now ready to return to the consideration of Eq. (10). We shall suppose that the integers x, y, z, t contain no common factor other than unity. Then at least one of them is odd. If t is even one of the numbers x, y, z is even; suppose it is x. Then y^2+z^2 is divisible by 4 and hence y and z are even. Then x, y, z, t have the common factor 2 contrary to hypothesis. Hence t is odd. Then one of the numbers x, y, z is odd. Suppose it is x. Then y^2+z^2 is divisible by 4 and hence y and z are even.

Now write Eq. (10) in the form

$$(t-x)(t+x)=y^2+z^2. \tag{17}$$

Suppose that $t-x$ and $t+x$ have a common odd prime factor r in common, where r is of the form $4n+3$. Then r is a factor of $(t-x)+(t+x)$, and hence of t, and hence likewise of x, while

$$y^2+z^2\equiv 0 \bmod r. \tag{18}$$

If z is not divisible by r then there exists an integer z_1 such that

$$zz_1\equiv 1 \bmod r.$$

(See the author's *Theory of Numbers*, p. 43.) Hence

$$(yz_1)^2+1\equiv 0 \bmod r.$$

But this is impossible, since -1 is a quadratic non-residue of every prime number of the form $4n+3$. Hence, z, and therefore y, is divisible by r. Then x, y, z, t have the common

factor r, contrary to hypothesis. Hence $t-x$ and $t+x$ have no common prime factor of the form $4n+3$.

If congruence (18) is verified we have just seen that y and z are both divisible by r. Hence from (17) it follows that if either $t-x$ or $t+x$ contains a factor r of the form $4n+3$ it contains that factor to an even power. From this result and the foregoing lemmas it follows at once that integers m, n, p, q exist such that

$$t+x=2(m^2+q^2), \quad t-x=2(n^2+p^2),$$

since both $t-x$ and $t+x$ are even. Hence t and x have the form given in (11), while

$$y^2+z^2=4(m^2+q^2)(n^2+p^2).$$

Since y and z are even it now follows readily from the corollary to lemma III that for a given t, x, y, z the integers m, n, p, q may be so chosen that y and z are representable in the form given in (11).

Hence we conclude that formulæ (11) afford the general integral solution of Eq. (10) if each of the second members is multiplied by the arbitrary integral factor d.

EXERCISES

1. By means of equations (5), (6), (7) find values of ξ, η, μ, ν such that

$$\{g(x, y, u, v)\}^3=g(\xi, \eta, \mu, \nu).$$

Apply this result to the solution of each of the equations

$$\xi^2+a\eta^2+b\mu^2+ab\nu^2=t^3, \quad \xi^2+a\eta^2+b\mu^2=t^3,$$

finding a four-parameter solution of the former and a one-parameter solution of the latter. Here ξ, η, μ, ν, t are the integers to be determined.

2. Obtain an eight-parameter solution of the equation

$$x^2+ay^2+bu^2+abv^2=x_1^2+ay_1^2+bu_1^2+abv_1^2,$$

where x, y, u, v, x_1, y_1, u_1, v_1 are the integers to be determined.

3. Obtain a six-parameter solution of the equation

$$x^2+ay^2+bz^2=u^2+av^2+bw^2,$$

where x, y, z, u, v, w are the integers to be determined.

4. Find an integral solution of the equation

$$x^2+y^2+z^2=u^2+v^2+w^2=r^2+s^2+t^2,$$

involving at least four independent parameters.

5. Find an integral solution of the equation

$$x^2+2y^2=u^2+v^2+w^2,$$

containing at least two arbitrary parameters.

6. Given a relation of the form

$$A^2+B^2+C^2=k(a^2+b^2+c^2),$$

where A, B, C, a, b, c, k are integers and $aB \neq bA$; find a one-parameter solution of the equation

$$x^2+y^2+z^2=k(u^2+v^2+w^2).$$

Find several values of k, less than 100, and the corresponding integers A, B, C, a, b, c such that the first equation stated in this problem is satisfied. In particular, show that k may have the values $k=7$, 19, 67. (Realis, 1882.)

§ 11. Certain Equations of Higher Degree

Let us consider the equation

$$\alpha^4+a\beta^4+b\gamma^4=\mu^2, \tag{1}$$

where α, β, γ, μ are the integers to be determined. As the form of the first member of this equation defines a set of numbers which do not form a domain with respect to multiplication, we shall naturally seek to extend the set in such way that the resulting class of integers do form a domain with respect to multiplication. For this purpose let us replace α^2, β^2, γ^2 by x, y, u respectively and adjoin the new variable v so as to give rise to the class of numbers defined by the form

$$x^2+ay^2+bu^2+abv^2.$$

This class forms a domain with respect to multiplication, as we have already seen.

Concerning this extension let us observe that the set of numbers $\alpha^4+a\beta^4+b\gamma^4$ have been extended simultaneously in two different ways. One way is by the generalization of variables already present; the other is by the adjunction of a new variable. We have here, then, an example of two methods of extending a set of numbers. These methods we shall find of frequent use and great importance in the theory of Diophantine equations.

Let us return now to Eq. (1) and consider it in connection with the group (7) of equations in the preceding section. By

means of the first equation in that group (with v taken equal to zero) we see that (1) will be satisfied if

$$\left.\begin{aligned} \mu &= x^2+ay^2+bu^2, \\ \alpha^2 &= x^2-ay^2-bu^2, \\ \beta^2 &= 2xy, \\ \gamma^2 &= 2ux. \end{aligned}\right\} \tag{2}$$

Here x, y, u are integers to be so restricted that (2) shall be satisfied.

From the last equation in group (7), already referred to, we see that the second equation in (2) will be satisfied if

$$\left.\begin{aligned} \alpha &= x_1^2-ay_1^2-bu_1^2, \\ x &= x_1^2+ay_1^2+bu_1^2, \\ y &= 2x_1y_1, \\ u &= 2u_1x_1. \end{aligned}\right\} \tag{3}$$

Then the third and fourth equations in (2) become

$$\left.\begin{aligned} \beta^2 &= 4x_1y_1(x_1^2+ay_1^2+bu_1^2), \\ \gamma^2 &= 4u_1x_1(x_1^2+ay_1^2+bu_1^2). \end{aligned}\right\} \tag{4}$$

These can be satisfied if we have

$$\left.\begin{aligned} &x_1=x_2^2, \quad y_1=y_2^2, \quad u_1=u_2^2, \\ &x_2^4+ay_2^4+bu_2^4=\rho^2. \end{aligned}\right\} \tag{5}$$

The last equation in (5) is of the same form as (1). Hence if we know a single solution of (1), we can by its means satisfy the last equation in (5). Then from the remaining Eqs. (5) and Eqs. (2), (3), (4), we can determine values of α, β, γ, μ. Therefore, from a single solution of (1) we can find a second solution; from this one a third can be obtained; from the third a fourth can be gotten; and so on. Thus we have at hand a means for determining in general an infinite number of solutions of (1) as soon as a single solution is known.

As an illustration of this method let us consider the special equation in which $a=b=2$, namely, the equation,

$$\alpha^4+2\beta^4+2\gamma^4=\mu^2.$$

A particular solution is afforded by the relation

$$3^4+2\cdot 4^4+2\cdot 2^4=25^2.$$

Associating this with Eq. (5), we see that we may take $x_2=3$, $y_2=4$, $u_2=2$, $\rho=25$. Then we have $x_1=9$, $y_1=16$, $u_1=4$; whence from (3) we have $\alpha=-463$, $x=625$, $y=288$, $u=72$. Thence from (2) we see that

$$\alpha=463, \quad \beta=600, \quad \gamma=300, \quad \mu=566{,}881$$

is a second solution of the equation. From this a third may be obtained in a similar manner; and so on *ad infinitum*.

Let us now consider the equation

$$\alpha^2+a\beta^2+b\gamma^2=\mu^4. \tag{6}$$

Again making use of Eqs. (7) of the preceding section we see that (6) will be satisfied if

$$\left.\begin{aligned} \mu^2&=x^2+ay^2+bu^2+abv^2,\\ \alpha&=x^2-ay^2-bu^2+abv^2,\\ \beta&=2xy-2buv,\\ \gamma&=2ux+2avy. \end{aligned}\right\} \tag{7}$$

It is only the first equation of this set which puts a condition on the integers x, y, u, v. That equation will be satisfied if

$$\left.\begin{aligned} \mu&=x_1^2+ay_1^2+bu_1^2+abv_1^2,\\ x&=x_1^2-ay_1^2-bu_1^2+abv_1^2,\\ y&=2x_1y_1-2bu_1v_1,\\ u&=2u_1x_1+2av_1y_1,\\ v&=0. \end{aligned}\right\} \tag{8}$$

Here x_1, y_1, u_1, v_1 are arbitrary integers. Hence Eqs. (7) and (8) afford a four-parameter solution of Eq. (6).

Finally, let us consider the equation

$$\alpha^4+a\beta^4=\mu^2+b\nu^2. \tag{9}$$

There is often a measure of choice at our disposal concerning the set of numbers which we shall extend to form a domain

with respect to multiplication. Here we may extend the set determined by either of the following forms:

$$\alpha^4+a\beta^4-b\nu^2, \quad \mu^2+b\nu^2-a\beta^4.$$

We shall employ the latter alone.

Proceeding as in the previous cases, we may write

$$\left.\begin{aligned} \alpha^2 &= x^2+by^2-au^2, \\ \mu &= x^2-by^2+au^2, \\ \nu &= 2xy, \\ \beta^2 &= 2ux. \end{aligned}\right\} \tag{10}$$

To satisfy the first of these equations it is sufficient to take

$$\left.\begin{aligned} \alpha &= x_1^2+by_1^2-au_1^2, \\ x &= x_1^2-by_1^2+au_1^2, \\ y &= 2x_1y_1, \\ u &= 2u_1x_1. \end{aligned}\right\} \tag{11}$$

Then from the last equation in (10) we have the further restriction:

$$\beta^2 = 4u_1x_1(x_1^2-by_1^2+au_1^2).$$

This can be satisfied if we write

$$\left.\begin{aligned} u_1 &= u_2^2, \quad x_1 = x_2^2; \\ x_2^4+au_2^4-by_1^2 &= \rho^2. \end{aligned}\right\} \tag{12}$$

But this last equation is of the same form as (9). Hence from a single solution of (9) we have integers satisfying the last equation in (12). From these we can determine a second solution of (9) by means of Eqs. (10), (11), (12). From this a third can be found; and so on.

As a special case of (9) consider the equation

$$\alpha^4+\beta^4 = \mu^2+\nu^2,$$

which has a solution afforded by the relation

$$6^4+5^4 = 39^2+20^2.$$

Comparing with (12) and remembering that we now have $a=b=1$, we see that we may take $x_2=6$, $u_2=5$, $y_1=20$ (or y_1 might be taken equal to 39 and thus another result be finally obtained). Then $x_1=36$, $u_1=25$. Thence from (11) one may determine x, y, u and thence from (10) values of α, β, μ, ν may be found which will satisfy the relation $\alpha^4+\beta^4=\mu^2+\nu^2$. From this second solution a third may be found; and so on *ad infinitum*.

Many other equations of the sort treated in this section are amenable to the same methods. Some of these are indicated in the general exercises at the close of this chapter.

EXERCISES

1. Show how to find an infinite number of integral solutions of the equation

$$\alpha^4+a\beta^4=\mu^2,$$

from a single given integral solution. Find several values of a for which integral solutions certainly exist.

2. Obtain a two-parameter integral solution of the equation

$$\alpha^2+a\beta^2=\mu^4.$$

3. Show how to find a two-parameter integral solution of the equation

$$\alpha^2+a\beta^2=\mu^n,$$

for any given positive integral value of n.

§ 12. On the Extension of a Set of Numbers so as to Form a Multiplicative Domain

In the preceding sections of this chapter we have instances illustrating a matter of great importance in Diophantine analysis. It is intimately connected with the fact that certain classes of integers form a domain with respect to multiplication. We have seen how the properties of such a domain may be employed to obtain solutions of a considerable class of equations. Moreover, we have found it profitable to generalize a set of integers introduced by a given equation so that the resulting set shall form a domain, whereas the original set did not. In the first place we extended the given set by the

adjunction of a new variable; this method can evidently be generalized, when convenient, by the introduction of two or more variables. In the second place we extended the given set by the generalization of variables already present. These are two widely useful methods of extension which may be employed either separately or simultaneously. They serve to unify and connect many problems which otherwise would appear unrelated.

If a given equation is put forward for consideration it is usually a matter of ingenuity to determine a suitable method of extension so as to give rise to a domain with respect to multiplication; and it is not at all improbable that no method will be apparent. In fact, it is easy to propose problems which are not yet amenable to solution either by this or by other means. There are, however, certain general classes of equations to which the method will apply, and these will be indicated as we proceed.

But the chief value of the method of extension does not consist so much in its use for the solution of equations proposed at random, as in its use for the arrangement of large and interesting classes of problems in an order in which they are amenable to attack and for suggesting a uniform procedure by which they may be investigated. One cannot fail to see the value of this in accomplishing the desirable end of building up a considerable body of connected doctrine.

There is one general case in which the extension by the adjunction of new variables is possible and to which we wish to direct attention. We begin with an illustration.

Suppose that a problem gives rise to the set of numbers x^3+y^3. They do not form a domain with respect to multiplication. Let us consider the product

$$P(x, y, z) = (x+y+z)(x+\omega y+\omega^2 z)(x+\omega^2 y+\omega z), \qquad (1)$$

where ω and ω^2 are the imaginary cube roots of unity. By multiplication we find that

$$P(x, y, z) = x^3+y^3+z^3-3xyz. \qquad (2)$$

Hence $P(x, y, 0) = x^3+y^3$. Hence the set of numbers $P(x, y, z)$ is an extension of the set x^3+y^3.

Now

$$(x+\omega y+\omega^2 z)(u+\omega v+\omega^2 w) = r+\omega s+\omega^2 t, \tag{3}$$

where

$$\left.\begin{aligned} r &= xu+yw+zv, \\ s &= xv+yu+zw, \\ t &= xw+yv+zu. \end{aligned}\right\} \tag{4}$$

Hence

$$P(x, y, z)\cdot P(u, v, w) = P(r, s, t).$$

Therefore, the numbers $P(x, y, z)$ form a domain with respect to multiplication.

By interchanging the role of v and w we have also

$$P(x, y, z)\cdot P(u, v, w) = P(r_1, s_1, t_1), \tag{5}$$

where

$$\left.\begin{aligned} r_1 &= xu+yv+zw, \\ s_1 &= xw+yu+zv, \\ t_1 &= xv+yw+zu. \end{aligned}\right\} \tag{6}$$

Let us consider more generally the set of numbers

$$x_1^n+a_1x_1^{n-1}x_2+a_2x_1^{n-2}x_2^2+\ldots+a_{n-1}x_1x_2^{n-1}+a_nx_2^n, \tag{7}$$

where $a_1, a_2, \ldots, a_n$ are given quantities. The method of extending this set so that the resulting set shall form a domain with respect to multiplication grows out of a remark due to Lagrange (*Œuvres*, Vol. VII, pp. 164–179), though Lagrange seems nowhere to have utilized it in connection with Diophantine problems. A partial use of it has been made by Legendre (*Théorie des nombres*, Vol. II, 3d edition, pp. 134–141); but its consequences seem nowhere to have been systematically developed.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of the equation

$$t^n-a_1t^{n-1}+a_2t^{n-2}-\ldots+(-1)^{n-1}a_{n-1}t+(-1)^n a_n = 0. \tag{8}$$

Form the product

$$P(x) = \prod_{i=1}^{n}(x_1+\alpha_i x_2+\alpha_i^2 x_3+\ldots+\alpha_i^{n-1}x_n). \tag{9}$$

This is a symmetric function of the roots of Eq. (8), whence we see readily that it may be written as a homogeneous polynomial of the nth degree in the quantities $x_1, x_2, \ldots, x_n$ with coefficients which are polynomials in $a_1, a_2, \ldots, a_n$, the latter having integral coefficients. For $x_3 = x_4 = \ldots = x_n = 0$, it is clear that $P(x)$ is identical with the expression in (7). Hence the set of numbers (7) is extended into the set (9) by the adjunction of the new variables $x_3, x_4, \ldots, x_n$.

It remains to show that the numbers $P(x)$ form a domain with respect to multiplication. Let $P(x)$ and $P(y)$ be two numbers of the form (9). Then we have

$$P(x) \cdot P(y) = \prod_{i=1}^{n} (x_1 + \alpha_i x_2 + \ldots + \alpha_i^{n-1} x_n)(y_1 + \alpha_i y_2 + \ldots + \alpha_i^{n-1} y_n). \quad (10)$$

Let us multiply together the two quantities

$$x_1 + \alpha_i x_2 + \ldots + \alpha_i^{n-1} x_n, \quad y_1 + \alpha_i y_2 + \ldots + \alpha_i^{n-1} y_n,$$

and in the product repeatedly replace α_i^{n+k}, $k \geqq 0$, by its value

$$\alpha_i^{n+k} = a_1 \alpha_i^{n+k-1} - a_2 \alpha_i^{n+k-2} + a_3 \alpha_i^{n+k-3} - \ldots, \quad k \geqq 0,$$

until the result is reduced to the form

$$z_1 + \alpha_i z_2 + \alpha_i^2 z_3 + \ldots + \alpha_i^{n-1} z_n,$$

where $z_1, z_2, \ldots, z_n$ are determinate polynomials in $x_1, \ldots, x_n, y_1, \ldots, y_n$. Then it is obvious that we have

$$P(x) \cdot P(y) = P(z); \quad (11)$$

that is, the product of two numbers of the given form is itself of the same form. Hence the numbers $P(x)$ form a domain with respect to multiplication.

It is obvious that one can obtain immediately an n-parameter solution of the equation

$$P(x) = t^k,$$

where k is any positive integer. For this purpose it is sufficient to write $t = P(z)$ and to determine $x_1, \ldots, x_n$ from the relation

$$\{P(z)\}^k = P(x).$$

Again, from a single solution of the equation

$$P(x)=0,$$

an n-parameter solution may be obtained by means of Eq. (11), $y_1, \ldots, y_n$ being taken as arbitrary and the quantities $z_1, \ldots, z_n$ being the new values of $x_1, \ldots, x_n$.

In a similar manner, from a single solution of the equation

$$P(x)=1, \tag{12}$$

others may be found. From a solution of Eq. (12) and a solution of the equation

$$P(x)=m,$$

other solutions of the latter may obviously be obtained.

GENERAL EXERCISES

1. If p, q, r satisfy the relations

$$p+q+r=1, \quad \frac{1}{p}+\frac{1}{q}+\frac{1}{r}=0,$$

show that

$$a^2+b^2+c^2=(pa+qb+rc)^2+(qa+rb+pc)^2+(ra+pb+qc)^2.$$

(Davis, 1912.)

2. Obtain solutions of the equation

$$(x^2+y^2+z^2)(x_1^2+y_1^2+z_1^2)=u^2+v^2+w^2.$$

(Catalan, 1893.)

3. By means of the identity

$$(a_1^2+a_2^2+\ldots+a_n^2)^2 \equiv (a_1^2+a_2^2+\ldots+a^2{}_{n-1}-a_n^2)^2+(2a_1a_n)^2+(2a_2a_n)^2+\ldots+(2a_{n-1}a_n)^2$$

show how to find any number of square numbers whose sum is a square.

(Martin, 1896.)

4 Show how to write the square of a sum of n squares as a sum of n squares.

(Moureaux, 1894.)

5. By means of the identities

$$(1+a+b+ab+a^2+b^2)^2 \equiv (1+a)^2(a+b)^2+(1+b)^2(a+b)^2+(1+a+b-ab)^2$$
$$\equiv a^2(a+b+1)^2+b^2(a+b+1)^2+(a+b+1)^2+(a+b+ab)^2,$$

show how to separate certain squares into a sum of three and of four squares.

(Avillez, 1897.)

6.* Show how to find other solutions of the system

$$x^2-by^2=u^2, \quad x^2+by^2=v^2,$$

when a single solution is known. Prove that a non-trivial solution does not exist when b is a square number. Show further that a necessary and sufficient condition for the existence of an integral solution is that integers m, n, p exist, such that

$$bp^2=mn(m+n)(m-n). \qquad \text{(Lucas, 1876.)}$$

7.* Discuss the solution of the Diophantine system

$$x^2+xy+2y^2=u^2,\quad x^2-xy-2y^2=v^2. \qquad \text{(Lucas, 1876.)}$$

8.* Show how to find a second solution of the system

$$2v^2-u^2=w^2,\quad 2v^2+u^2=3z^2,$$

when a single solution is known; thence find the general solution of the system.
(Lucas, 1877; Pepin, 1879.)

9.* Show that the only integral solution of the system

$$2v^2-u^2=w^4,\quad 2v^2+u^2=3z^2,$$

is the trivial one in which each of the numbers u, v, w, z is equal to ± 1.
(Lucas, 1877.)

10. Let p, r, s be three numbers satisfying the relation

$$r^4+ar^2s^2+bs^4=p^2.$$

Show that the equation

$$x^4+ax^2y^2+by^4=z^2$$

has the further solution

$$x=r^4-bs^4,\quad y=2prs,\quad z=p^4-(a^2-4b)r^4s^4.$$

Derive this result by a direct use of the method of extension by generalization of variables. (Lebesgue, 1853.)

11.* Prove that the equation

$$x^4-2^my^4=1$$

is impossible in positive integers x, y, m. (Thue, 1903.)

12.* Determine the values of m for which the equation

$$x^4+mx^2y^2+y^4=z^2$$

has non-trivial solutions. (Werebrüssov, 1908.)

13.† Determine the integral values of m and n for which the equation

$$x^4+mx^2y^2+ny^4=z^2$$

has non-trivial solutions.

14.† Investigate further the problem of solving the equation

$$x^2+ay^2+bz^2=t^k$$

for integral values of k greater than 2.

15.† Investigate the problem of solving the system

$$x^2+y^2+z^2=k(u^2+v^2+w^2)=l(r^2+s^2+t^2)$$

for particular values of k and l. (Compare Exs. 4 and 6 in § 10.)

16.† Develop in further detail the theory of the equation

$$x^4+ay^4+bz^4=t^2.$$

(See special cases of this equation in Chapter IV.)

17.† Investigate the problem of solving the equation

$$x^4+ay^4+bz^4=t^k$$

for integral values of k greater than 2. In particular, consider the case $k=4$.

18.† Investigate the problem of solving the equation

$$x^4+ay^4=u^2+av^2.$$

19.† Develop in further detail the theory of the equation

$$x^4+ay^4=u^2+bv^2.$$

20.† Investigate the problem of solving the equation

$$x^4+ay^4+bu^4+abv^4=t^2.$$

21.† Let a, b, k be given integers, k being positive. Investigate the properties of the integer m such that the equation

$$x^2+axy+by^2=mt^k$$

shall possess integral solutions and find these solutions when they exist. In particular, treat the cases $k=2$, $k=3$.

22.† Develop a similar theory for each of the following equations:

$$x^2+ay^2+bz^2=mt^k,$$

$$x^4+ay^4+bz^4=mt^k,$$

$$x^4+ay^4=m(u^2+av^2),$$

$$x^4+ay^4=m(u^2+bv^2).$$

CHAPTER III

EQUATIONS OF THE THIRD DEGREE

§ 13. On the Equation $kx^3+ax^2y+bxy^2+cy^3=t^2$

We shall now consider the problem of finding solutions of the equation

$$x^3+ax^2y+bxy^2+cy^3=t^2, \tag{1}$$

where a, b, c are rational numbers. By our general method (in §12) of extending the set of numbers defined by the first member we are led to consider the function

$$h(\alpha, \beta, \gamma)=\prod_{i=1}^{3}(\alpha+\rho_i\beta+\rho_i^2\gamma), \tag{2}$$

where ρ_1, ρ_2, ρ_3 are the roots of the equation

$$\rho^3-a\rho^2+b\rho-c=0. \tag{3}$$

It is obvious that $h(x, y, 0)=x^3+ax^2y+bxy^2+cy^3$.

Performing the requisite multiplications, we have

$$h(\alpha, \beta, \gamma)=\alpha^3+a\alpha^2\beta+b\alpha\beta^2+c\beta^3+(a^2-2b)\alpha^2\gamma+(b^2-2ac)\alpha\gamma^2 \\ +ac\beta^2\gamma+bc\beta\gamma^2+c^2\gamma^3+(ab-3c)\alpha\beta\gamma. \tag{4}$$

Since ρ_i satisfies Eq. (3), it is easy to see that we have a relation of the form

$$(\alpha+\rho_i\beta+\rho_i^2\gamma)(u+\rho_iv+\rho_i^2w)=r+\rho_is+\rho_i^2t,$$

where r, s, t are rational. On computing the values of r, s, t, we are led to the following result:

I. *If r, s, t have the values*

$$\left.\begin{aligned} r&=\alpha u+c\gamma v+c\beta w+ac\gamma w,\\ s&=\beta u+\alpha v-b\gamma v-b\beta w+c\gamma w-ab\gamma w,\\ t&=\gamma u+\beta v+\alpha w+a\gamma v+a\beta w-b\gamma w+a^2\gamma w,\end{aligned}\right\} \tag{5}$$

then

$$h(\alpha, \beta, \gamma)\cdot h(u, v, w)=h(r, s, t). \tag{6}$$

From this formula we see readily that

$$\{h(\alpha, \beta, \gamma)\}^2 = h(\alpha^2 + 2c\beta\gamma + ac\gamma^2, \quad 2\alpha\beta - 2b\beta\gamma + c\gamma^2 - ab\gamma^2, \\ 2\alpha\gamma + \beta^2 + 2a\beta\gamma - b\gamma^2 + a^2\gamma^2). \quad (7)$$

By means of the last relation we are able to find a two-parameter solution of Eq. (1). The latter we may write in the form $h(x, y, 0) = t^2$. Comparing this with Eq. (7) we see that a solution is afforded by the values

$$\left.\begin{aligned} t &= h(\alpha, \beta, \gamma), \\ x &= \alpha^2 + 2c\beta\gamma + ac\gamma^2, \\ y &= 2\alpha\beta - 2b\beta\gamma + c\gamma^2 - ab\gamma^2, \end{aligned}\right\} \quad (8)$$

provided that α, β, γ are connected by the relation

$$2\alpha\gamma + \beta^2 + 2a\beta\gamma - b\gamma^2 + a^2\gamma^2 = 0. \quad (9)$$

Into the last relation α enters linearly. It is therefore a rational function of β and γ with rational coefficients. Hence,

II. *A two-parameter rational solution of* (1) *is afforded by the set* (8) *where* β *and* γ *are arbitrary rational numbers (except that* γ *must in general be different from zero) and* α *is determined by Eq.* (9).

If we set $\gamma = 2m$, $\beta = 2mn$, where m and n are integers, we are led immediately to the following result:

III. *If* a, b, c *are integers, then a two-parameter integral solution of* (1) *is afforded by the values*

$$t = h(\alpha, 2mn, 2m),$$
$$x = \alpha^2 + 8cm^2n + 4acm^2,$$
$$y = 4\alpha m - 8bm^2n + 4cm^2 - 4abm,^2$$

where

$$\alpha = bm - a^2m - 2amn - mn^2,$$

m and n being arbitrary integers.

It is obvious that these results may be applied readily to the solution of the equation

$$kx^3 + ax^2y + bxy^2 + cy^3 = t^2, \quad k \neq 0; \quad (10)$$

for, if this equation is multiplied through by k^2 and kx is replaced by x, the resulting equation is of the form of (1).

The reader may readily supply numerical illustrations of these results.

A method of finding particular solutions of Eq. (10) is due to Fermat. It applies only when k or c is a square. Let us suppose that k is a square. Write the equation in the form

$$d^2x^3+ax^2y+bxy^2+cy^3=t^2. \tag{11}$$

Take $x=1$ and set

$$t=d+\frac{a}{2d}y.$$

Then we have

$$\left(d+\frac{a}{2d}y\right)^2+\left(b-\frac{a^2}{4d^2}\right)y^2+cy^3=\left(d+\frac{a}{2d}y\right)^2.$$

This gives

$$y=\frac{1}{c}\left(\frac{a^2}{4d^2}-b\right).$$

From this value of y we have a value of t, and hence a solution of (11).

§ 14. On the Equation $kx^3+ax^2y+bxy^2+cy^3=t^3$

If we set

$$\left.\begin{aligned} u&=\alpha^2+2c\beta\gamma+ac\gamma^2,\\ v&=2\alpha\beta-2b\beta\gamma+c\gamma^2-ab\gamma^2,\\ w&=2\alpha\gamma+\beta^2+2a\beta\gamma-b\gamma^2+a^2\gamma^2,\end{aligned}\right\} \tag{1}$$

then from Eqs. (5), (6), (7) of the preceding section we see that

$$\{h(\alpha,\beta,\gamma)\}^3=h(\rho,\sigma,\tau), \tag{2}$$

where

$$\left.\begin{aligned} \rho&=\alpha u+c\gamma v+c\beta w+ac\gamma w,\\ \sigma&=\beta u+\alpha v-b\gamma v-b\beta w+c\gamma w-ab\gamma w,\\ \tau&=\gamma u+\beta v+\alpha w+a\gamma v+a\beta w-b\gamma w+a^2\gamma w.\end{aligned}\right\} \tag{3}$$

For a solution of the equation

$$x^3+ax^2y+bxy^2+cy^3=t^3, \tag{4}$$

it is obviously sufficient to take

$$t=h(\alpha,\beta,\gamma),\quad x=\rho,\quad y=\sigma,\quad \tau=0. \tag{5}$$

Hence the equation $\tau = 0$ puts the necessary restriction on the otherwise arbitrary quantities α, β, γ.

Since τ is the crucial quantity, let us write out its value in terms of α, β, γ. We have

$$\tau = 3\alpha^2\gamma + 3\alpha\beta^2 + 3(a^2-b)\alpha\gamma^2 + 2(a^3+3a-ab)\alpha\beta\gamma + a\beta^3 + 3(a^2-b)\beta^2\gamma + (a^3-4ab+3c)\beta\gamma^2 + (a^4-3a^2b+2ac+b^2)\gamma^3. \quad (6)$$

From any solution of the equation $\tau = 0$ we have a solution of (4).

In order that the equation $\tau = 0$ shall determine a rational value of α, it is obviously necessary and sufficient that the expression

$$\{3\beta^2 + 3(a^2-b)\gamma^2 + 2(a^3+3a-ab)\beta\gamma\}^2 - 12\gamma\{a\beta^3 + 3(a^2-b)\beta^2\gamma + (a^3-4ab+3c)\beta\gamma^2 + (a^4-3a^2b+2ac+b^2)\gamma^3\},$$

shall be equal to a square. If we call this m^2, we have

$$9\beta^4 + 12(a^3+2a-ab)\beta^3\gamma + 2(2a^6+12a^4-4a^4b+9a^2-12a^2b+2a^2b^2+9b)\beta^2\gamma^2 + 12(a^5+3a^4-a^3-2a^3b+ab+ab^2-3c)\beta\gamma^3 + (-a^4+6a^2b-b^2-8ac)\gamma^4 = m^2. \quad (7)$$

A method of finding in general an infinite number of solutions of this equation is given in § 17 of the following chapter. The work done here consists essentially in reducing the problem of solving Eq. (4) to that of solving Eq. (7).

A particular solution of Eq. (7) is obvious. It is gotten by setting $\gamma = 0$. This gives rise to the following solution of (4):

$$t = 2a^3 - 9ab + 27c,$$
$$x = 27c - a^3,$$
$$y = 9a^2 - 27b.$$

But this particular solution is more readily obtained by the method of Fermat described below.

The equation

$$k^3x^3 + ax^2y + bxy^2 + cy^3 = t^3, \quad (8)$$

can be readily reduced to the form of (4). It is sufficient to multiply the equation through by k^6 and replace x by k^3x. Hence the previously developed theory is applicable to Eq. (8).

Another method of effecting a reduction similar to that above is the following (see Schaewen, *Jahresbericht der Deutschen Mathematiker-Vereinigung*, Vol. XVIII, pp. 7–14): In the general equation (8) replace x by

$$kx-\frac{a}{3k^2}y.$$

Then we have a result which may be written

$$k^3x^3+pxy^2+qy^3=t^3. \tag{9}$$

This equation may be put in the form

$$(t-kx)(t^2+kxt+k^2x^2)=y^2(px+qy).$$

The last equation will be satisfied if one writes

$$m(t-kx)=ny,$$

$$n(t^2+kxt+k^2x^2)=m(pxy+qy^2),$$

where m and n are arbitrary quantities. If we put

$$t-kx=\frac{n}{m}y,$$

the first of these equations is satisfied while the second becomes

$$3k^2m^2nx^2-(pm^3-3kmn^2)xy-(qm^3-n^3)y^2=0.$$

If we denote the discriminant of this equation by $m^2\rho^2$ we see that it, and hence Eq. (9), has a rational solution which may be immediately derived as soon as one knows rational numbers m, n, ρ, satisfying the equation

$$p^2m^4+12k^2qm^3n-6kpm^2n^2-3k^2n^4=\rho^2. \tag{10}$$

Thus we have reduced the problem of solving Eq. (9) to that of solving Eq. (10).

There is an interesting method by which particular solutions of Eq. (4), and, in fact, of the more general equation

$$Ax^3+Bx^2y+Cxy^2+Dy^3=t^3, \tag{11}$$

may often be obtained (see Schaewen, *l. c.*). It depends essentially on writing Eq. (11) in the form

$$P^3+Q=t^3, \tag{11 bis}$$

where P is a linear expression in x and y and Q is a polynomial which has at least one rational linear factor. A convenient pair of values of x and y can be chosen so as to reduce such a linear factor to zero. Then t can readily be found. Thus a particular solution of (11) is obtained. The applicability of this method depends on whether or not Eq. (11) may conveniently be thrown into the form (11 bis).

As an example, we take the equation

$$x^3-5x^2y-6xy^2+8y^3=t^3. \tag{12}$$

It may be written in each of five forms as follows:

$$8y^3+x(x+y)(x-6y)=t^3,$$

$$x^3-(x+2y)(5x-4y)y=t^3.$$

$$\left(x-\frac{5}{3}y\right)^3-\frac{y^2}{27}(387x-341y)=t^3,$$

$$(x+2y)^3-xy(11x+18y)=t^3,$$

$$\left(2y-\frac{x}{2}\right)^3+\frac{x^2}{8}(9x-52y)=t^3.$$

These give rise to the following pairs of values of x and y, each of which affords a solution of Eq. (12), namely: $x=1$, $y=-1$; $x=6$, $y=1$; $x=2$, $y=-1$; $x=4$, $y=5$; $x=341$, $y=387$; $x=18$, $y=-11$; $x=52$, $y=9$.

A special case of this method is due to Fermat. Suppose that $A=a^3$. Then for P we may take

$$P=ax+\frac{B}{3a^2}y.$$

Then Q has the factor y^2 and hence a linear factor. Thus one has a solution in all cases when A is a cube. Similarly there is a solution when t is a cube. It must be observed that for special equations this method may lead only to a trivial solution of the given equation. This is true in the case of an equation in the form $x^3+cy^3=t^3$.

It may be remarked that the problem of finding integral solutions of Eq. (11) is obviously equivalent to that of finding rational solutions of the equation

$$Ax^3+Bx^2+Cx+D=t^3; \tag{13}$$

for (11) is reduced to (13) by dividing it through by y^3 and in the resulting equation writing x, t for x/y, t/y, respectively. It is in this latter form that the problem was investigated by Fermat and Euler.

Fermat observed that from a single solution of Eq. (13) others can usually be obtained. The method is as follows: Let $x=m$ afford a rational solution of (13) and let $t=s$ be the corresponding value of t. Then in (13) replace x by $\xi+m$. The equation takes the form

$$A\xi^3+\overline{B}\xi^2+\overline{C}\xi+s^3=t^3. \tag{14}$$

Now if we write

$$t=s+\frac{\overline{C}}{3s^2}\xi,$$

we can readily determine a rational value of ξ, in general different from zero, such that Eq. (14) is satisfied. Adding m to this value of ξ, we have a new value of x which affords a solution of (13). Starting from this new value of x we can usually determine a third; and so on indefinitely. For certain particular equations the method may fail to lead to new solutions. This will be the case when the solution obtained for (14) is $\xi=0$, $t=s$.

As an illustrative example, let us consider the equation

$$x^3-5x^2+x+4=t^3.$$

This has the solution $x=1$, $t=1$. Then write $x=\xi+1$, whence the equation takes the form

$$\xi^3-2\xi^2-6\xi+1=t^3.$$

Putting $t=1-2\xi$ in the last equation and solving the resulting equation for ξ we have $\xi=14/9$. Thence, as a second solution of our given equation, we have $x=23/9$, $t=-19/9$. From this second solution a third may be found; and so on indefinitely.

For an investigation concerning the existence of a solution of Eq. (13), see Haentzschel, *Jahresbericht der Deutschen Mathematiker-Vereinigung*, Vol. XXII, pp. 319–329.

§ 15. On the Equation

$$x^3+y^3+z^3-3xyz=u^3+v^3+w^3-3uvw$$

Probably the most elegant particular equations of the third degree are the following:

$$x^3+y^3=u^3, \tag{1}$$

$$x^3+y^3=u^3+v^3. \tag{2}$$

That the former is impossible in integers different from zero will be shown in the next section. The general solution of the latter we shall derive in this section. It is convenient to consider first the more general equation

$$x^3+y^3+z^3-3xyz=u^3+v^3+w^3-3uvw. \tag{3}$$

This equation reduces to (2) on putting $z=w=0$. Moreover, it is the equation to which one is led on extending each of the two sets of integers $x^3 \mid y^3$, $u^3 \mid v^3$ so as to arrive at a multiplicative domain, as one sees by reference to § 12. (It may be observed that the problem of finding integral solutions of (2) and (3) and that of finding rational solutions are essentially the same.)

Let us denote the first member of (3) by $P(x, y, z)$ as in § 12. Then from Eqs. (3) to (6) in § 12 we see that

$$P(r, s, t)\cdot P(m, n, p)=P(x, y, z)=P(u, v, w),$$

where

$$\left.\begin{aligned} x&=mr+nt+ps,\\ y&=ms+nr+pt,\\ z&=mt+ns+pr, \end{aligned}\right\} \tag{4}$$

and

$$\left.\begin{aligned} u&=mr+ns+pt,\\ v&=mt+nr+ps,\\ w&=ms+nt+pr. \end{aligned}\right\} \tag{5}$$

Eqs. (4) and (5) afford a six-parameter solution of (3). This solution, so readily obtained, unfortunately lacks generality.

We proceed as follows to find a more general solution: Write Eq. (3) in the form

$$(x+y+z)(x^2+y^2+z^2-xy-yz-zx) = (u+v+w)(u^2+v^2+w^2-uv-vw-wu).$$

We may exclude as trivial the cases in which each member is equal to zero; for all such solutions are obtained readily by means of linear equations. (Compare the factorization of $P(x, y, z)$ in § 12.) Then we may write

$$\frac{x+y+z}{u+v+w} = \frac{u^2+v^2+w^2-uv-vw-wu}{x^2+y^2+z^2-xy-yz-zx}.$$

Now put

$$u=w+\alpha, \quad v=w+\beta, \quad x=z+\gamma, \quad y=z+\delta. \tag{6}$$

Then we have

$$\frac{x+y+z}{u+v+w} = \frac{\alpha^2-\alpha\beta+\beta^2}{\gamma^2-\gamma\delta+\delta^2}. \tag{7}$$

Multiplying both numerator and denominator of the fraction in the second member of (7) by the denominator we may write the result in the form

$$\frac{x+y+z}{u+v+w} = \frac{{\alpha_1}^2-\alpha_1\beta_1+{\beta_1}^2}{(\gamma^2-\gamma\delta+\delta^2)^2} = {\alpha_2}^2-\alpha_2\beta_2+{\beta_2}^2,$$

where α_2 and β_2 are rational numbers, when u, v, w, x, y, z are rational numbers. Compare formula (2) in § 7.

If we write

$$a=\frac{\alpha_2+\beta_2}{2}, \quad b=\frac{\alpha_2-\beta_2}{2},$$

then the preceding equation takes the form

$$x+y+z=(a^2+3b^2)(u+v+w). \tag{8}$$

Hence, for every rational solution x, y, z, u, v, w of Eq. (3) rational numbers a and b exist such that Eq. (8) is satisfied.

From Eqs. (7) and (8) we have

$$(a^2+3b^2)(\gamma^2-\gamma\delta+\delta^2)=\alpha^2-\alpha\beta+\beta^2.$$

This relation may be put in the form

$$(a^2+3b^2)\left[\left(\frac{\gamma+\delta}{2}\right)^2+3\left(\frac{\gamma-\delta}{2}\right)^2\right]=\left(\frac{\alpha+\beta}{2}\right)^2+3\left(\frac{\alpha-\beta}{2}\right)^2. \quad (9)$$

By means of the relation

$$(a^2+3b^2)(c^2+3d^2)\equiv(ac+3bd)^2+3(ad-bc)^2$$

we see that Eq. (9) is satisfied if we have

$$\left.\begin{aligned} a(\gamma+\delta)+3b(\gamma-\delta)&=\alpha+\beta,\\ a(\gamma-\delta)-\ b(\gamma+\delta)&=\alpha-\beta.\end{aligned}\right\} \quad (10)$$

From the homogeneous character of Eq. (3) it follows that if each of the numbers x, y, z, u, v, w in a particular rational solution is divided or multiplied by a given rational number, the resulting numbers form a rational solution. Hence without loss of generality we may take $u+v+w$ equal to unity. This we do. Then, in view of (7), we have

$$u+v+w=1,$$
$$x+y+z=a^2+3b^2;$$

and thence from (6),

$$\left.\begin{aligned} \alpha+\beta&=1-3w,\\ \gamma+\delta&=a^2+3b^2-3z.\end{aligned}\right\} \quad (11)$$

Eqs. (10) and (11) may now be solved for α, β, γ, δ. If the results are put in Eq. (6), we have

$$\left.\begin{aligned} x&=\frac{-(a-3b)(a^2+3b^2-3z)+1-3w}{6b}+z,\\ y&=\frac{(a+3b)(a^2+3b^2-3z)-1+3w}{6b}+z,\\ u&=\frac{-(a^2+3b^2)(a^2+3b^2-3z)+(a+3b)-3w(a+3b)}{6b}+w,\\ v&=\frac{(a^2+3b^2)(a^2+3b^2-3z)-(a-3b)+3w(a-3b)}{6b}+w,\end{aligned}\right\} \quad (12)$$

while z and w are arbitrary. This affords a rational solution of (3) depending upon four rational parameters.

Setting $z=w=0$ and multiplying the resulting values of x, y, u, v by $6b$, we are led to the following solution of Eq. (2):

$$\left.\begin{aligned} x&=-(a-3b)(a^2+3b^2)+1,\\ y&=(a+3b)(a^2+3b^2)-1,\\ u&=-(a^2+3b^2)^2+(a+3b),\\ v&=(a^2+3b^2)^2-(a-3b). \end{aligned}\right\} \tag{13}$$

This solution is due to Euler and Binet; they obtained it by a different method.

We shall now show that formulæ (13) afford the general solution of Eq. (2) (exclusive of trivial solutions) except for an arbitrary constant k multiplying the second member of each equation in (13). In doing this it is convenient, first of all, to transform the solution in the following manner: Put

$$a=\frac{\rho+\sigma}{2m},\quad b=\frac{\sigma-\rho}{6m},\quad n=\frac{\rho^2+\rho\sigma+\sigma^2}{3m}.$$

(This transformation is employed by Fujiwara in *Arch. Math. Phys.* (3) 19 (1912): 369. See other papers referred to in this note.) On replacing x, y, u, v by m^2 times their former values, we may write the resulting solution in the form:

$$x=-n\rho+m^2,\quad y=n\sigma-m^2,\quad u=m\sigma-n^2,\quad v=-m\rho+n^2. \tag{14}$$

Here ρ, σ, m, n are arbitrary parameters except for the relation

$$\rho^2+\rho\sigma+\sigma^2=3mn. \tag{15}$$

To prove that (14) affords the general solution of (2) it is obviously sufficient to show how to determine ρ, σ, m, n so as to satisfy Eqs. (14) and (15) when x, y, u, v, in order, are replaced by a suitable multiple of any given set of values satisfying (2). For this purpose we may proceed thus (see Schwering, *Arch. Math. Phys.* (3) 2 (1902): 281):

From (14) we have

$$x+y=n(\sigma-\rho),\quad u+v=m(\sigma-\rho);$$

whence

$$\frac{m}{n}=\frac{u+v}{x+y}.$$

Therefore, we may write

$$m=\lambda(u+v), \quad n=\lambda(x+y). \tag{16}$$

Now again from (14) we have

$$nv-mx=n^3-m^3.$$

If in this equation we substitute the values of m, n from Eq. (16), we have

$$\lambda^2=\frac{v(x+y)-x(u+v)}{(x+y)^3-(u+v)^3}.$$

Since the numerator and denominator here are homogeneous, the former of degree 2 and the latter of degree 3, it is obvious that this equation will be satisfied by $\lambda=1$, provided that x, y, u, v are replaced by τx, τy, τu, τv, respectively, and τ is suitably determined. Replacing them by these same multiples in Eqs. (14) and (16) we see that (16) affords the values of m and n and that (14) affords the values of ρ and σ.

It remains to show that Eq. (15) is satisfied. This we do by substituting in Eq. (2) the values of x, y, u, v taken from (14). Thus we have

$$(-n\rho+m^2)^3+(n\sigma-m^2)^3+(-m\sigma+n^2)^3+(m\rho-n^2)^3=0.$$

Hence

$$(m^3-n^3)(\rho-\sigma)(\rho^2+\rho\sigma+\sigma^2-3mn)=0.$$

Therefore Eq. (15) one of the relations $m=n$, $\rho=\sigma$ is satisfied. If $m=n$ then $x=v$, $y=u$. If $\rho=\sigma$, then $x=-y$, $u=-v$. Hence, except in the case of trivial solutions, Eq. (15) is satisfied. Therefore, Eqs. (14), with the condition (15), afford the general solution of (2). Likewise Eqs. (13) afford the general solution of (2). In each case the elements of the solution given are all to be multiplied by an arbitrary constant k.

If in (13) we set $a=0$, $b=\frac{1}{2}$, and multiply the resulting values of x, y, u, v by 16, we are led to the relation

$$34^3+2^3=15^3+33^3,$$

as a particular case of the sum of two cubes equal to the sum of two other cubes.

§ 16. Impossibility of the Equation $x^3+y^3=2^m z^3$

We shall first consider the foregoing equation for the case $m=0$; it then has the form

$$x^3+y^3=z^3. \tag{1}$$

In order to prove that this equation is impossible in integers x, y, z, all of which are different from zero, we shall have need of some lemmas similar to those in § 10. We shall now state them and indicate the means of proof.

Lemma I. *If a number is expressible in the form $\alpha^2+3\beta^2$, and if the quotient $(\alpha^2+3\beta^2)/(a^2+3b^2)$ is an integer m, where α, β, a, b are integers and a^2+3b^2 is a prime number, then m is expressible in the form $\gamma^2+3\delta^2$, where γ and δ are integers.*

Lemma II. *Every prime number of the form $6n+1$ can be represented in one and in only one way in the form a^2+3b^2 where a and b are integers. No prime number of the form $6n-1$ is a divisor of a number of the form a^2+3b^2 where a and b are relatively prime.*

Lemma III. *Let p be a prime number of the form $6n+1$ and write $p=a^2+3b^2$, where a and b are integers. Let m be any integer such that $pm=\alpha^2+3\beta^2$, where α and β are integers. Then there exists a representation of m as a sum of two integral squares,*

$$m=\left(\frac{a\alpha\pm 3b\beta}{a^2+3b^2}\right)^2+3\left(\frac{\alpha b\mp a\beta}{a^2+3b^2}\right)^2, \tag{2}$$

such that the representation $\alpha^2+3\beta^2$ of pm is obtained from the foregoing representations of p and m by multiplication in accordance with the formula

$$(a^2+3b^2)(c^2+3d^2)=(ac+3bd)^2+3(ad-bc)^2.$$

Corollary. *If h is a composite number all of whose prime factors are of the form $6n+1$ and if we write $h=h_1h_2$, where h_1 and h_2 are positive integers, then every representation of h in the form a^2+3b^2 is obtained by taking every representation of h_1 and h_2 and multiplying these expressions in accordance with the formula*

$$(a^2+3b^2)(c^2+3d^2)=(ac\pm 3bd)^2+3(ad\mp bc)^2.$$

The proof of lemma I is obtained by an obvious modification of that of lemma I in § 10. The proof of lemma II is a close parallel to that of lemma II in § 10; in this case, however, one starts from the fact that -3 is a quadratic residue of primes of the form $6n+1$ and of no other odd primes. The proof of lemma III is like that of lemma III in § 10. The reader can readily supply the necessary argumentation in all cases.

Our immediate use of these lemmas is in finding the general solution of the equation

$$p^2+3q^2=s^3, \tag{3}$$

where p and q are relatively prime integers and s is odd. It is clear that s must have the form

$$s=t^2+3u^2, \tag{4}$$

where t and u are integers. Writing $(t^2+3u^2)^3$ in the form p^2+3q^2 by means of a repeated use of the last formula in the foregoing corollary, we have

$$p=t^3-9tu^2, \quad q=3u(t^2-u^2). \tag{5}$$

Eqs. (4) and (5) give all the integral solutions of (3) subject to the condition that p and q are relatively prime and s is odd.

Let us now return to Eq. (1). Our method of proof (see Euler, *Opera Omnia*, series 1, Vol. I, pp. 484–489) is to assume that Eq. (1) is satisfied by a set of numbers x, y, z, all of which are different from zero, and to prove that we are then led to a contradiction. Let d be the greatest common divisor of any two of these numbers. It is then a divisor of the third. Eq. (1) may then be divided through by d^3 and a new equation of the same form obtained in which the resulting x, y, z are prime each to each. Hence, without loss of generality, we may assume that Eq. (1) itself is satisfied by integers x, y, z which are prime each to each; and this we do. Then it is easy to see that two of the numbers x, y, z are odd and the other one even. We shall assume that x and y are odd. This assumption involves no loss of generality, since if one of these numbers, say x, is even, then the other, in this case y, may be

transposed to the second member so that we have $x^3 = z^3 + (-y)^3$, an equation of the same form as (1), in which the two numbers in the same member are both odd.

Let us now write

$$x+y=2p, \quad x-y=2q.$$

Then $x=p+q$, $y=p-q$, so that p and q are relatively prime integers, one of them being odd and the other even. Substituting in (1), we have

$$2p(p^2+3q^2)=z^3. \tag{6}$$

From this equation it is clear that p is even, since p^2+3q^2 is odd; hence q is odd. Since p and q are relatively prime it follows that p and p^2+3q^2 have the greatest common divisor 1 or 3. We treat these two cases separately.

In the first place suppose that p and p^2+3q^2 have the greatest common divisor 1. Then p is not divisible by 3. Then from Eq. (6) we have

$$2p=r^3, \quad p^2+3q^2=s^3. \tag{7}$$

We have seen above that the last equation can be satisfied only when p and q have the values given in (5). Since q is odd it follows from the last equation in (5) that u is odd and t is even. From the first equation in (5) we see that t is not divisible by 3. Moreover, t and u are relatively prime, since the same is true of p and q. From the two values of p above we have the relation

$$(2t)(t+3u)(t-3u)=r^3.$$

It is clear that the three factors in the first member are prime each to each. Hence each of them is a cube. Writing them in order equal to the cubes μ^3, ρ^3, σ^3, we have

$$\rho^3+\sigma^3=\mu^3. \tag{8}$$

It is easy to verify that the numbers ρ, σ are less in absolute value than the numbers x, y with which we set out. Moreover, both of them are odd. Furthermore, μ is different from zero.

Let us now consider the case in which p and p^2+3q^2 have

the greatest common divisor 3. Then write $p = 3\pi$. Then from Eq. (6) we have

$$6\pi = 9r^3, \quad 9\pi^2 + 3q^2 = 3s^3;$$

or

$$2\pi = 3r^3, \quad q^2 + 3\pi^2 = s^3.$$

Here we see that π is even. Hence q is odd. In view of (5) as the general solution of (3) we see that q and π have the forms

$$q = t^3 - 9tu^2, \quad \pi = 3u(t^2 - u^2).$$

Since π is even it follows from the last equation that u is even and t is odd. From the two values of π we have

$$(2u)(t+u)(t-u) = r^3.$$

It is clear that the three factors in the first member of this equation are prime each to each. From this we are led as before to an equation of the form (8) with the same properties as in the preceding case.

Therefore, starting with an equation $x^3 + y^3 = z^3$ in which x, y, z are all different from zero and are prime each to each and x and y are odd, we are led to another equation $x_1^3 + y_1^3 = z_1^3$ of the same sort, in which x_1, y_1 are less in absolute value than x, y. Starting from the last equation, we can proceed as before to an equation $x_2^3 + y_2^3 = z_2^3$ with the same properties as in the preceding case, x_2, y_2 being less in absolute value than x_1, y_1; and so on. But such a recursion is evidently impossible. From this contradiction we conclude that *Eq.* (1) *cannot be satisfied by integers* x, y, z, *all of which are different from zero.*

Let us now turn to the equation

$$x^3 + y^3 = 2^m z^3. \tag{9}$$

In view of the result just attained, this is impossible in non-zero integers x, y, z if m is a multiple of 3; hence we shall not consider this case further. It is clear that x and y are both odd or both even; if they are both even, it is clear that the equation may be divided through by an appropriate power of 2, so that in the resulting equation x and y shall be both odd. This may necessitate a change in the value of m. After

x and y are made odd, we suppose that m is so chosen that z also is odd. We shall now show that *the equation in this reduced form is impossible in non-zero integers, except for the trivial solution* $x=y=z$, *which exists when* $m=1$. It is obviously sufficient to prove this for the case when x and y are relatively prime.

Eq. (9) may be written in the form

$$(x+y)(x^2-xy+y^2)=2^m z^3.$$

The two factors of the first member have the greatest common divisor 1 or 3 since x and y are to be taken relatively prime. Hence the factor x^2-xy+y^2 is of one of the forms r^3, $3r^3$. For the former case we may write

$$x^2-xy+y^2=\left(\frac{x+y}{2}\right)^2+3\left(\frac{x-y}{2}\right)^2=r^3, \quad x+y=2^m s^3, \quad (10)$$

where r and s are odd integers. In the latter case we have

$$x^2-xy+y^2=\left(\frac{x+y}{2}\right)^2+3\left(\frac{x-y}{2}\right)^2=3r^3, \quad x+y=2^m 3^2\cdot s^3\cdot$$

or

$$\left(\frac{x-y}{2}\right)^2+3\left(\frac{x+y}{6}\right)^2=r^3, \quad x+y=2^m\cdot 3^2\cdot s^3. \quad (11)$$

We shall merely outline the remainder of the proof. Consider Eqs. (10). From the first of these and the theory associated with Eq. (3) above, we have equations of the form

$$r=t^2+3u^2, \quad \frac{x+y}{2}=t^3-9tu^2, \quad \frac{x-y}{2}=3u(t^2-u^2).$$

Thence from the second equation in (10), we have

$$t(t-3u)(t+3u)=2^{m-1}s^3.$$

Now t^2+3u^2 is odd, being equal to the odd integer r. Hence t^2-9u^2 is odd. From the last equation it follows then that t has the factor 2^{m-1}. Thence we have equations of the form

$$t=2^{m-1}\mu^3, \quad t-3u=\alpha^3, \quad t+3u=\beta^3,$$

and hence the relation

$$\alpha^3+\beta^3=2^m\mu^3.$$

Similarly, by means of Eq. (11), one is led again to an equation of this last form. In each case it may be shown that the integers involved in the deduced equation are smaller than those in (9), and hence the conclusion announced above is reached by the Fermatian method of infinite descent.

GENERAL EXERCISES

1. Prove that the sum of the sixth powers of two integers cannot be the square of an integer.

2. Prove that no integers x and y exist such that the difference of their sixth powers is a square.

3. Prove that no relatively prime integers x and y exist such that the difference of their fourth powers is a cube.

4. Show that the equation $x^6+y^6=z^6$ is impossible in non-zero integers.

5. By means of the identity

$$(a^2-b^2+cd)^2+(ad+bc)^2+(b^2-c^2+ad)(a^2-b^2-cd)=(a^2+b^2)(c^2+d^2)^2$$

show that the Diophantine equation $x^2+y^2=z^3$ has rational solutions (for which $z\neq 0$) when and only when n satisfies an equation of the form

$$an^2=a(a+1).$$

6.* If p and q denote numbers of the form $12n+5$ and $12n+11$ respectively, and if s is a number of any one of the forms p, p^2, q, q^2, pq, qp^2, pq, pq^2, p^2, $4p^2$, $4q^2$, $4pq$; then neither of the equations

$$x^3+y^3=nz^3, \quad xy(x+y)=nz^3,$$

has a non-trivial rational solution.

(For reference to several papers dealing with these equations see *Encyclopédie des sciences mathématiques*, Tome I, Vol. III, pp. 32–33.)

7. By means of a single solution of the equation $x^2+y^2=u^2+v^2$ show directly how to find a two-parameter solution.

8.* Obtain the general solution of the Diophantine system

$$x^3+y^3=u^3+v^3=z^3+t^3. \qquad \text{(Werebrüssow, 1900.)}$$

9. Show that the equation $x^2+y^2+z^2=w^2$ is satisfied by $x=u+v$, $y=u-v$, $w=u^2+v^2$, $z=2uv$; $x=u^2-v^2$, $y=2uv$, $z=u^2+v^2$, $w=u$. By means of two solutions show how to find a third. (Werebrüssow, 1908.)

10. By means of a single solution of the equation $x^2+y^2+w^2=t^2$ show how to find a two-parameter solution. Generalize the result by increasing the number of variables in the first member.

11. Consider the equation $1+x+x^2+x^3=y^5$. Show that $x=7$, $y=20$ is the only solution in which x is a prime number. Show how to find other rational solutions. (Gerono, 1877.)

12. Show that no one of the following four equations has an integral solution:

$$2x^3\pm 1=z^3, \quad 2x^3\pm 2=z^3. \qquad \text{(Delannoy, 1897.)}$$

13. Let $x=\alpha$, $y=\beta$, $z=\gamma$ be a solution of the equation $x^3+y^3=pz^3$. Show that another solution is obtained by means of the formulæ

$$x=\alpha(\alpha^3+2\beta^3),\quad y=-\beta(2\alpha^3+\beta^3),\quad z=\gamma(\alpha^3-\beta^3).$$

Obtain a similar result for the equation $x^3+y^3=pz^3$. (Realis, 1878.)

14. Show that the equation $x+y+z=xyz$ has an integral solution except $x=y=0$, $x=y=1$.

15. Show that the equation $3x^3+1=y^3$ has an integral solution except $x=0$, $y=1$; $x=1$, $y=2$.

16. By means of a single solution of the equation $x^3+ay^3=bz^3$ show how to find a second; by means of this find a third; and so on. (Legendre.)

17. Find a two-parameter integral solution of the equation $x^3+y^3=z^2$.

18. Find a three-parameter integral solution of the equation $x^3+2y^3=u^3+v^3$.

Suggestion.—Observe that

$$u^3+v^3=(u+v)\left\{\left(\frac{u+v}{2}\right)^2+3\left(\frac{u-v}{2}\right)^2\right\}.$$

19. Obtain solutions of the equation $x^3+y^3=u^3+v^3$.

20. Find three parameter solutions of the equation $x^3+y^3+z^3=u^3+v^3$.

Suggestion.—Employ the identity

$$(-a+b+c)^3+(a-b+c)^3+(a+b-c)^3-(a+b+c)^3=24abc.$$

21. Obtain a three parameter solution of the equation

$$x^3+y^3+z^3=3xyz=u^3+3v^3.$$

22. Find the general integral solution of the equation $t^2=x^3+y^3+1$.

23. Construct another cubic equation for which large classes of solutions may be found by the first method employed in § 15. Develop the theory of this equation.

24. Investigate the properties of the integer m such that the equation

$$x^3+y^3+z^3-3xyz=mt^3$$

shall have solutions and find solutions involving arbitrary parameters (when m is suitably determined). Treat the corresponding problems for the simpler equation $x^3+y^3=mt^3$.

25. Generalize the investigations called for in the preceding problem by treating the more general equation

$$h(x,y,z)=mt^3,$$

the function h being defined as in Eq. (4) of § 13.

26. From $3^3+4^3+5^3=6^3$ deduce $7^3+14^3+17^3=20^3$.

CHAPTER IV

EQUATIONS OF THE FOURTH DEGREE*

§ 17. On the Equation $ax^4+bx^3y+cx^2y^2+dxy^3+ey^4=mz^2$

For the equation

$$ax^4+bx^3y+cx^2y^2+dxy^3+ey^4=mz^2, \tag{1}$$

it is obvious that the problem of finding rational solutions and that of finding integral solutions are essentially equivalent. It will therefore be sufficient to consider only one of these problems; it is convenient to treat the former rather than the latter. If the equation is multiplied through by m and mz is then replaced by z we have a new equation of the form which (1) takes on replacing m by unity. We shall therefore consider only the case when $m=1$. Now it is clear that the problem of finding rational solutions of (1) is equivalent to that of finding rational solutions of the equation

$$ax^4+bx^3+cx^2+dx+e=z^2; \tag{2}$$

for if (1) is divided through by y^4 and in the result x is put for $x:y$ and z for $z:y^2$, m having been replaced by 1, we have an equation of the form (2). We shall confine our attention to the reduced equation (2).

The customary method of finding rational solutions of Eq. (2) is due to Fermat. It takes different forms for different cases. We shall examine these cases separately.

Suppose that e is a square number, say $e=\epsilon^2$. Then write

$$z=mx^2+nx+\epsilon,$$

where m and n are rational numbers subject to our choice.

* Other matter relating to equations of the fourth degree is to be found in § 11 and in the exercises at the close of Chapter II.

They are to be determined so that the value of z^2, namely,

$$z^2 = m^2x^4 + 2mnx^3 + (n^2 + 2me)x^2 + 2nex + e^2,$$

shall coincide with the first member of Eq. (2) except for the terms in x^4 and x^3. For this it is necessary and sufficient that

$$n = \frac{d}{2e}, \quad m = \frac{c}{2e} - \frac{d^2}{8e^3},$$

Then we have

$$ax^4 + bx^3 = m^2x^4 + 2mnx^3,$$

an equation which is satisfied if

$$x = \frac{b - 2mn}{m^2 - a}.$$

Thus we have in general a single rational solution of Eq. (2).

As an illustration, it may thus be shown that the equation

$$x^4 + 3x^3 + 5x^2 + 2x + 1 = z^2,$$

has the solution $\qquad x = -\frac{1}{8}, \quad z = \frac{7}{8}.$

In case a is a square number, say $a = \alpha^2$, we may write

$$z = \alpha x^2 + mx + n,$$

and proceed in a manner similar to that employed in the preceding paragraph. Here we choose m and n so as to make the expression for z^2 coincide with the first member of (2) except for the independent term and the term containing x, and then determine x as before. We have

$$m = \frac{b}{2\alpha}, \quad n = \frac{c}{2\alpha} - \frac{b^2}{8\alpha^3}, \quad x = \frac{n^2 - e}{d - 2mn}.$$

Here again we have in general a single rational solution of Eq. (2).

If one applies this method to the particular equation

$$x^4 + 3x^3 + 5x^2 + 2x + 1 = z^2,$$

one finds that a solution is afforded by $x = -37/136$.

If both a and e are squares, say $a = \alpha^2$ and $e = \epsilon^2$, we may write,

$$z = \alpha x^2 + mx + \epsilon,$$

and then determine m so that the expression for z^2 shall coincide with the first member of Eq. (2) except for the terms

containing x^3 and x^2 or the terms containing x^2 and x. These lead in order to the following pairs of values of m and x:

$$m=\frac{d}{2e},\quad x=\frac{c-m^2-2ve}{2am-b};$$

$$m=\frac{b}{2a},\quad x=\frac{d-2me}{m^2+2ae-c}.$$

Here we have in general two solutions of Eq. (2).

By means of the equation

$$x^4+3x^3+5x^2+2x+1=z^2$$

the reader may readily supply a numerical illustration of this method.

Gathering together the results thus obtained we may say that we have a method which in general is effective for finding a single rational solution of (2) when c is a square or when a is a square and for finding two rational solutions when both a and e are squares.

We shall now show that Eq. (2) may be reduced to one of the special forms already considered provided that a single rational solution is known.

Let $x=k$, $z=p$ be a rational solution of Eq. (2). Then replace x by $t+k$. It is clear that a new equation is obtained of the same form as (2) and that p^2 is the constant corresponding to e. Since this constant is a square, the first method employed above may be used to find a solution of the new equation. Adding k to the resulting value of t we have a value of x which affords a rational solution of Eq. (2). This in general is different from the solution with which we started. By means of this second solution a third can in general be obtained; by means of this a fourth, and so on. Hence, if a single rational solution of (2) is known it is possible in general to find as many as may be desired.

As an illustrative example, consider the equation

$$2x^4+5x^3+7x^2+2=z^2.$$

It has the solution

$$x=1,\quad z=4.$$

If we replace x by $t+1$ the new equation takes the form

$$2t^4+13t^3+34t^2+37t+16=z^2,$$

the constant term 16 being a square number. A solution of the last equation may be found by the methods indicated above. By means of this a second solution of the equation in x is readily obtained. With this in hand, the operation may be repeated and thus a third solution of the equation in x be obtained; and so on *ad infinitum*.

EXERCISES

1. Determine integral Pythagorean triangles such that the hypotenuse and the sum of the legs shall be squares. (Compare Ex. 4 of § 3.) (Fermat.)

2. Determine integral Pythagorean triangles such that the hypotenuse and the difference of the legs shall be squares.

3. Find two or more pairs of integral Pythagorean triangles such that in each pair the difference of the legs of one shall be equal to the difference of the legs of the other while the longer leg of one is equal to the hypotenuse of the other.

4. Find two or more pairs of integral Pythagorean triangles such that in each pair the sum of the legs of one shall be equal to the sum of the legs of the other, while the hypotenuse of one shall be equal to the greater leg of the other.

§ 18. On the Equation $ax^4+by^4=cz^2$

The equation

$$ax^4+by^4=cz^2, \tag{1}$$

which is a special case of that considered in the preceding section, has been treated by several authors and detailed investigations have been given of special cases, that is, of certain special equations obtained by giving to a, b, c particular values. No attempt will be made to summarize these investigations. On the other hand, an exposition will be given of a new method of attack which leads to solutions in an important class of cases. Convenient references to a representative part of the literature concerning Eq. (1) may be found in *Encyclopédie des sciences mathématiques*, Tome I, Vol. III, pp. 35–36, and in *Jahrbuch über die Fortschritte der Mathematik*, at places indicated by the following volume and page numbers: 10: 146, 148; 11: 136, 137; 12: 131, 136; 14: 133; 16: 154; 19: 187; 21: 181; 25: 295; 26: 211, 212.

If Eq. (1) is multiplied through by a^3 and ax is then replaced by x, an equation is obtained which is of the form

$$x^4+my^4=nz^2. \tag{2}$$

It is in this latter form that we shall treat the equation. We shall suppose m to be any given integer and shall then restrict n to be an integer of the form s^4+mt^4, where s and t are integers. Then Eq. (2) takes the form

$$x^4+my^4=(s^4+mt^4)z^2. \tag{3}$$

Here m, s, t are given integers and x, y, z are unknown integers suitable values of which are to be sought.

It should be observed that there is no real loss of generality in confining n to this form; for if Eq. (2) has a solution, then there is a square number ρ^2 such that $n\rho^2$ has the form s^4+mt^4.

Since $x=s$, $y=t$, $z=1$ is a solution of (3) we might proceed to find another as in the work of the preceding section. We shall, however, use a different method. Let us write z in the form

$$z=p^2+mq^2, \tag{4}$$

and seek to determine p and q and corresponding to them values of x and y satisfying Eq. (3). We have

$$\begin{aligned} x^4+my^4&=(s^4+mt^4)(p^2+mq^2)^2\\ &=(s^4+mt^4)\{(p^2-mq^2)^2+m(2pq)^2\}\\ &=\{s^2(p^2-mq^2)+2mt^2pq\}^2+m\{t^2(p^2-mq^2)-2s^2pq\}^2. \end{aligned}$$

This equation will be satisfied if x^2 and y^2 have the values

$$\left.\begin{aligned} x^2&=s^2(p^2-mq^2)+2mt^2pq,\\ y^2&=t^2(p^2-mq^2)-2s^2pq. \end{aligned}\right\}. \tag{5}$$

The last two equations form a system of the type studied by Fermat under the name *double equations*, x, y, p, and q being the unknown integers. We shall obtain solutions of them by means similar to those employed by Fermat.

Multiplying the first equation in (5) by t^2 and the second by s^2 and subtracting, we have

$$t^2x^2-s^2y^2=2(s^4+mt^4)pq.$$

This equation will be satisfied if we put

$$tx+sy=2stp, \quad tx-sy=\frac{(s^4+mt^4)q}{st}.$$

(Here the coefficient of p is chosen so as to be equal to twice the square root of the coefficient of p^2 in the value of t^2x^2 obtained by multiplying the first equation in (5) through by t^2.) For x and y we have the values

$$x=sp+\frac{(s^4+mt^4)q}{2st^2},$$

$$y=tp-\frac{(s^4+mt^4)q}{2s^2t}.$$

If we use these values of x and y and determine p and q so that the first equation in (5) shall be satisfied, it is clear that the second equation is also satisfied.

Substituting the foregoing value of x in the first equation in (5) and reducing, we have

$$4s^2t^2(s^4+mt^4)pq+(s^4+mt^4)^2q^2=8ms^2t^6pq-4ms^4t^4q^2.$$

This equation will be satisfied if

$$p=(s^4+mt^4)^2+4ms^4t^4,$$

$$q=-4s^2t^2(s^4-mt^4).$$

Making use of these values of p and q, we have for x, y, z the values:

$$x=s\{(s^4+mt^4)^2+4ms^4t^4-2(s^8-m^2t^8)\},$$

$$y=t\{(s^4+mt^4)^2+4ms^4t^4+2(s^8-m^2t^8)\},$$

$$z=\{(s^4+mt^4)^2+4ms^4t^4\}^2+16ms^4t^4(s^4-mt^4)^2.$$

These values afford a single integral solution of Eq. (3). Employing this solution and utilizing the methods of the preceding section, one may obtain a second solution; from this in turn a third may be found; and so on. The reader may readily supply numerical illustrations.

EXERCISES

1. Obtain solutions of the equation $7x^4-5y^4=2z^2$. (Pepin, 1879.)

2. Obtain solutions of each of the following equations:

$$x^4-140y^4=z^2, \quad 4x^4-35y^4=z^2.$$ (Pepin, 1879.)

3. Obtain solutions of each of the following equations:

$$3x^4-2y^4=z^2, \quad x^4+7y^4=8z^2, \quad 7x^4-2y^4=5z^2.$$

(Pepin, 1879.)

4. Show how to find solutions of the equation $ax^4+by^4=cz^2$ in all cases in which $c=a+b$.

§ 19. Other Equations of the Fourth Degree

We have seen (§ 6) that the sum of two biquadrate numbers cannot be a biquadrate number; in fact, such a sum cannot be a square number. Furthermore, the sum of two biquadrates cannot be the double of a square number (Ex. 7 of § 6).

That the sum of three biquadrates can be a square is readily shown. Let x, y, z be integers such that

$$x^2+y^2=z^2. \tag{1}$$

Let us square each member of this equation, multiply through by z^4, and then add $x^4y^4-2z^4x^2y^2$ to each member of the resulting equation; the relation thus obtained may be written in the form

$$(xy)^4+(yz)^4+(zx)^4=(z^4-x^2y^2)^2. \tag{2}$$

Now Eq. (1) has the general primitive solution

$$x=m^2-n^2, \quad y=2mn, \quad z=m^2+n^2.$$

Substituting these values in (2) we have the identity

$$\{2mn(m^2-n^2)\}^4+\{2mn(m^2+n^2)\}^4+(m^4-n^4)^4 = (m^8+14m^4n^4+n^8)^2.$$

Thus we have a two-parameter solution of the problem of finding three biquadrate numbers whose sum is a square. If we put $m=2$, $n=1$, we have the particular illustrative relation $12^4+20^4+15^4=481^2$.

Whether or not the sum of three biquadrate numbers can be a biquadrate appears never to have been determined, though Euler seems to have been of the opinion that it is impossible.

It is easy to find three biquadrate numbers whose sum is equal to the double of a square. In fact, these are afforded by the identity

$$x^4+y^4+(x+y)^4=2(x^2+xy+y^2)^2. \tag{3}$$

Now the relation

$$x^2+xy+y^2=(a^2+ab+b^2)^2$$

is satisfied if

$$x=a^2-b^2, \quad y=2ab+b^2.$$

If we substitute these values of x and y in (3), we have the identity

$$(a^2-b^2)^4+(2ab+b^2)^4+(a^2+2ab)^4=2(a^2+ab+b^2)^4.$$

This affords a two-parameter solution of the problem of finding three biquadrate numbers whose sum is equal to the double of a biquadrate number. As a particular case we have

$$3^4+5^4+8^4=2\cdot 7^4.$$

In a similar way one may obtain an identity affording a two-parameter solution of the problem of finding three biquadrate numbers whose sum is the double of a number of any even power. For this purpose it is sufficient to determine x and y so that

$$x^2+xy+y^2=(a^2+ab+b^2)^k,$$

$2k$ being the index of the even power under consideration, and substitute the resulting values of x and y in (3). This determination of x and y may readily be made by the method set forth in § 7.

Whether the sum of four biquadrate numbers can be a biquadrate number appears not yet to have been determined. That the sum of five biquadrate numbers can be a biquadrate number is readily shown. The smallest integers satisfying this condition appear to be those involved in the relation

$$4^4+6^4+8^4+9^4+14^4=15^4.$$

Several identities affording a solution of this problem have been obtained by tentative methods. (See a paper by Martin

in the Proceedings of the International Congress of Mathematicians, 1912.) The following are two of them:

$$\left.\begin{aligned}&(8s^2+40st-24t^2)^4+(6s^2-44st-18t^2)^4\\&\qquad+(14s^2-4st-42t^2)^4+(9s^2+27t^2)^4\\&\qquad+(4s^2+12t^2)^4=(15s^2+45t^2)^4;\\&(4m^2-12n^2)^4+(2m^2-12mn-6n^2)^4+(4m^2+12n^2)^4\\&\qquad+(2m^2+12mn-6n^2)^4+(3m^2+9n^2)^4\\&\qquad=(5m^2+15n^2)^4\end{aligned}\right\}\tag{4}$$

Another elegant problem concerning biquadrate numbers is the following: To find two biquadrate numbers whose sum is equal to the sum of two other biquadrate numbers; in other words, to find solutions of the equation

$$x^4+y^4=u^4+v^4.\tag{5}$$

This problem we shall now consider. If we set

$$x=a+b,\quad y=c-d,\quad u=a-b,\quad v=c+d,\tag{6}$$

and substitute in Eq. (5), we have

$$ab(a^2+b^2)=cd(c^2+d^2).$$

Euler has observed that this equation is identically satisfied if

$$\begin{aligned}a&=g(f^2+g^2)(-f^4+18f^2g^2-g^4),\\b&=2f(f^6+10f^4g^2+f^2g^4+4g^6),\\c&=2g(4f^6+f^4g^2+10f^2g^4+g^6),\\d&=f(f^2+g^2)(-f^4+18f^2g^2-g^4).\end{aligned}$$

With these values of a, b, c, d, Eqs. (6) afford a two-parameter solution of (5).

Formulas for resolving the equation

$$x^4+y^4+z^4=u^4+v^4+w^4$$

have been given by several writers. See *Intermédiaire des Mathématiciens*, 19: 254; 20: 105. A two-parameter solution of the equation

$$w^4+x^4+y^4+z^4=s^4+t^4+u^4+v^4$$

may be found from Eqs. (4) above by putting $n=s$ and $m=3t$ and equating the first members, this being legitimate since the second members are identical.

GENERAL EXERCISES

1. Find a two-parameter solution of each of the following equations:

$$x^4+y^4+4z^4=t^4,$$

$$x^4+2y^4+2z^4=t^4,$$

$$x^4+8y^4+8z^4=t^4,$$

$$x^4+y^4+2z^4=2t^4,$$

$$x^4+y^4+8z^4=8t^4. \qquad \text{(Carmichael, 1913.)}$$

2. Obtain solutions of the equation

$$x^4+y^4+z^4=u^4+v^4.$$

3. Find six biquadrate numbers whose sum is a biquadrate.

4. Find n biquadrate numbers whose sum is a biquadrate in case $n=7$, 8, 9, 10.

5.* Show that $x=3$, $y=1$, $z=2$ are the only relatively prime integers which satisfy the equation

$$x^4-y^4=5z^4. \qquad \text{(Fauquembergue, 1912.)}$$

6. The equation $x(x+1)=2y^4$ has no integral solution other than $x=y=0$, $x=y=1$.

7. Starting from the equation $x^2+ay^2=z^2$ generalize the first result of § 19.

8.* Show how to find all the solutions of the equation $x^4+35y^4=z^2$ which lie under a given limit. (Pepin, 1895.)

9.* Show that the equation $px^4-41y^4=z^2$ has no rational solution when the prime p has any one of the values 5, 37, 73, 113, 337, 349, 353, . . ., represented by the form $5m^2+4mn+9n^2$. (This and several similar results are given by Pepin in the Comptes Rendus of the Paris Academy, Vol. LXXXVIII, pp. 1255–1257 and Vol. XCIV, pp. 122–124.)

10.* Obtain the general solution of the equation

$$x^4-8x^2y^2+8y^4=z^2. \qquad \text{(Pepin, 1898.)}$$

11.* Obtain formulæ affording solutions of the equation

$$ax^4+bx^2y^2+cy^4=dz^2. \qquad \text{(Aubry, 1911.)}$$

12.* Solve the equation

$$x^4+4hx^2y^2+(2h-1)^2y^4=z^2,$$

where h is such that $4h-1$ and $2h-1$ are primes. (Pietrocola, 1898.)

13. Obtain solutions of the equation

$$x^4+x^3y+x^2y^2+xy^3+y^4=z^2. \qquad \text{(Moret-Blanc, 1881.)}$$

14. Obtain solutions of the equation

$$x^4-5x^2y^2+5y^4=z^2. \qquad \text{(Moret-Blanc, 1881.)}$$

15.* Obtain the general solution of the equation $x^4-4x^2y^2+y^4=z^4$.
(Paraira, 1913.)

16. Obtain solutions of the equation

$$(x^2-y^2-2xy)^2-8x^2y^2=z^2. \qquad \text{(Aubry, 1913.)}$$

17.† Determine whether the sum of three biquadrate numbers can be equal to a biquadrate number.

18.† Determine whether the sum of four biquadrate numbers can be equal to a biquadrate number.

19.† Discuss the values of a for which the equation

$$x^4+y^4+a^2z^4=u^4$$

has non-zero integral solutions.

20.† Discuss the values of a (if any exist) for which the equation

$$x^4+a^2y^4+a^2z^4=u^4$$

has non-zero integral solutions.

CHAPTER V

EQUATIONS OF DEGREE HIGHER THAN THE FOURTH. THE FERMAT PROBLEM

§ 20. Remarks Concerning Equations of Higher Degree

When we pass to equations of degree higher than the fourth we find that but little effective progress has been made. Often it is a matter of great difficulty to determine whether a given solution is the general solution of a given equation. Indeed this is true, to a large extent, of equations of the third and fourth degrees. Even here there are but few equations for which a general solution is known or for which it is known that no solution at all exists. As the degree of the equation increases, the generality of the known results decreases in a rapid ratio. Only the most special equations of degree higher than the fourth have been at all treated and for only a few of these is one able to answer the questions naturally propounded as to the existence or generality of solutions. (See Ex. 71, p. 116.)

Several papers have been written on the problem of determining a sum of different nth powers equal to an nth power; but the methods employed are largely tentative in character and the results are far from complete. Reference may be made to Barbette's monograph of 154 quarto pages, entitled, "*Les sommes de $p^{ièmes}$ puissances distinctes égales à une $p^{ième}$ puissance*," and to a paper by A. Martin in the Proceedings of the International Congress of Mathematicians, 1912. See also the references in the latter paper.

It is an easy matter to construct equations of any degree desired in such a way that formulæ are readily obtained yielding rational solutions involving one or more parameters; but this is a trivial exercise. What is more profitable is a satisfactory treatment of those equations which first come to mind when

one considers the question as to what are the simplest equations of various given degrees. Probably the most elegant equation of degree n is the following:

$$x^n+y^n=z^n. \tag{1}$$

Concerning equations of higher degree the most desirable thing to do first is to ascertain methods by which one may treat completely the special cases, such, for example, as Eq. (1) above.

For a long time Eq. (1) has held an interesting place in the history and literature of the theory of numbers. This chapter is devoted principally to a study of that equation. It was first introduced to notice by Fermat in the seventeenth century. Fermat stated, without proof, the following theorem, commonly known as Fermat's Last Theorem:

If n is an integer greater than 2 there do not exist integers x, y, z, all different from zero, such that $x^n+y^n=z^n$.

This theorem was written down by Fermat on the margin of his copy of Diophantus. He added that he had discovered a truly remarkable proof of the theorem, but that the margin of the book was too narrow to contain it. No one has rediscovered Fermat's proof, if indeed he had one (and there seems to be no sufficient reason for doubting his statement). In fact, no general proof of the theorem has yet been found. For various special values of n proofs have been given; in particular for every value of n not greater than 100.

In the next section we shall develop the more elementary properties of Eq. (1); and in the following section we shall give a brief general account of the present state of knowledge concerning this equation.

§ 21. Elementary Properties of the Equation $x^n+y^n=z^n$, $n>2$

In the study of the equation

$$x^n+y^n=z^n, \quad n>2, \tag{1}$$

it is convenient to make some preliminary reductions. If there exists any particular solution of (1), there exists also

a solution in which x, y, z are prime each to each. This may be readily proved as follows: if any two of the numbers x, y, z have the greatest common factor d, then from (1) itself it follows that the third number of the set has also this same factor. Hence the equation may be divided through by d^n. The resulting equation is of the same form as (1). It is clear that x, y, z in this resulting equation are prime each to each. Hence, in proving the impossibility of (1), it is sufficient to treat only the case in which x, y, z are prime each to each.

Again, since n is greater than 2, it must contain the factor 4 or an odd prime factor p. If n contains the factor 4, we may write $n=4m$, whence we have

$$(x^m)^4+(y^m)^4=(z^m)^4.$$

From the corollary to theorem IV in § 5 it follows that this equation is impossible. Hence, if Eq. (1) is satisfied, n does not contain the factor 4. Now, if n contains the odd prime factor p, we may write $n=pm$, whence we have

$$(x^m)^p+(y^m)^p=(z^m)^p.$$

Therefore, in order to prove the impossibility of Eq. (1) it is sufficient to show that it is impossible when n is equal to an odd prime number p; that is, it is sufficient to prove the impossibility of the equation $x^p+y^p=z^p$, where p is an odd prime. By changing z to $-z$ this may be written in the more symmetric form

$$x^p+y^p+z^p=0. \tag{2}$$

We shall take x, y, z to be prime each to each.

Special proofs of the impossibility of Eq. (2) for particular values of p are known. One of these for the case $p=3$ has been reproduced in § 16 above. The remainder of this section is devoted to the derivation, by elementary means, of certain properties of x, y, z, p, which are necessary if Eq. (2) is to be satisfied.

We shall first derive the so-called Abelian formulæ. Let us write Eq. (1) in the form

$$(x+y)(x^{p-1}-x^{p-2}y+x^{p-3}y^2+\ldots-xy^{p-2}+y^{p-1})=(-z)^p. \tag{3}$$

The second factor of the first member of this equation may be written in the form

$$\frac{x^p+y^p}{x+y}=\frac{\{(x+y)-y\}^p+y^p}{x+y}$$
$$=\frac{(x+y)^p-p(x+y)^{p-1}y+\ldots+p(x+y)y^{p-1}}{x+y}$$
$$=(x+y)Q(x,y)+py^{p-1}, \qquad (4)$$

where $Q(x, y)$ is a polynomial in x and y with integral coefficients. From this and the fact that x and y are relatively prime, it follows readily that the numbers represented by the two factors in the first member of (3) have the greatest common divisor 1 or p.

If z is prime to p, this greatest common divisor must be 1. In this case the two factors of the first member of (3) are relatively prime. Then, since their product is a pth power, it is clear that each of them is a pth power. Hence we may write

$$x+y=u^p, \quad \frac{x^p+y^p}{x+y}=v^p, \quad z=-uv. \qquad (5)$$

Let us next consider the case in which z is divisible by p. Then $x^p+y^p\equiv 0 \bmod p$; thence, from the theorem of Fermat (see Carmichael's *Theory of Numbers*, p. 48), it follows that $x+y\equiv 0 \bmod p$. That is, $x+y$ has the factor p. Then, by means of Eq. (4), we see that the second factor in the first member of (3) also has the factor p. But the greatest common divisor of the two factors in the first member of (3) is 1 or p; therefore, in this case, it is p. Hence one of these two factors contains p to only the first power, while the other contains it to the $(kp-1)$th power, where k is a suitably determined positive integer. We shall show that it is the factor $x+y$ which contains p to the higher power. Suppose that $x+y$ contains the factor p to the νth power, and let us write

$$x+y=p^\nu t,$$

where t is prime to p. From this we have

$$x^p=(-y+p^\nu t)^p=-y^p+p^{\nu+1}ty^{p-1}-\frac{p-1}{2}p^{2\nu+1}t^2y^{p-2}+\ldots;$$

whence

$$x^p+y^p=p^{p+1}ty^{p-1}+p^{p+2}I,$$

where I is an integer. Now, in the case under consideration, y is prime to p, since by hypothesis, y is prime to z and z is divisible by p. Hence, x^p+y^p is divisible by p^{p+1}, but by no higher power of p. Therefore $(x^p+y^p)/(x+y)$ is divisible by p but not by p^2. Thence it follows that the first and second factors in the first member of (3) contain p^{kp-1} and p respectively. Therefore, we have relations of the form

$$x+y=p^{kp-1}u^p, \quad \frac{x^p+y^p}{x+y}=pv^p, \quad z=-p^kuv, \tag{6}$$

where k is a suitably chosen positive integer.

We can now readily prove the following theorems:

I. *If an equation of the form*

$$x^p+y^p+z^p=0, \tag{2 bis}$$

in which p is an odd prime, is satisfied by integers x, y, z, which are prime each to each and to p and are all different from zero, then integers u_1, u_2, u_3, v_1, v_2, v_3, prime to p, exist such that

$$\left.\begin{array}{lll} x+y=u_1^p, & \dfrac{x^p+y^p}{x+y}=v_1^p, & z=-u_1v_1, \\ y+z=u_2^p, & & x=-u_2v_2, \\ z+x=u_3^p, & & y=-u_3v_3; \end{array}\right\} \tag{7}$$

whence it follows that

$$\left.\begin{array}{l} x=\frac{1}{2}(u_1^p-u_2^p+u_3^p), \\ y=\frac{1}{2}(u_1^p+u_2^p-u_3^p), \\ z=\frac{1}{2}(-u_1^p+u_2^p+u_3^p). \end{array}\right\} \tag{8}$$

II. *If an equation of the form*

$$x^p+y^p+z^p=0, \tag{2 bis}$$

in which p is an odd prime, is satisfied by integers x, y, z, which are prime each to each, and if z is divisible by p, then integers u_1, u_2, u_3, v_1, v_2, v_3, prime to p, and a positive integer k, exist such that

$$\left.\begin{array}{lll} x+y=p^{kp-1}u_1^p, & \dfrac{x^p+y^p}{x+y}=pv_1^p, & z=-p^ku_1v_1, \\ y+z=u_2^p, & & x=-u_2v_2, \\ z+x=u_3^p, & & y=-u_3v_3; \end{array}\right\} \tag{9}$$

whence it follows that

$$\left.\begin{aligned} x &= \tfrac{1}{2}(p^{kp-1}u_1{}^p - u_2{}^p + u_3{}^p), \\ y &= \tfrac{1}{2}(p^{kp-1}u_1{}^p + u_2{}^p - u_3{}^p), \\ z &= \tfrac{1}{2}(-p^{kp-1}u_1{}^p + u_2{}^p + u_3{}^p). \end{aligned}\right\} \qquad (10)$$

To prove these theorems it is sufficient to show that formulæ (7) and (9) are true. The equations in the first line in (9) are equivalent to those in (6). The equations in the other two lines in (9) and in all three lines in (7) are essentially equivalent to those in (5), the only difference being in the interchange of the roles of x, y, z. This interchange is legitimate, since x, y, z enter symmetrically into Eq. (2^{bis}).

The formulæ contained in these theorems were given by Legendre (*Mém. Acad. d. Sciences, Institut de France*, 1823 [1827], p. 1). They are also to be found in a letter of Abel's to Holmboe and published in Abel's *Œuvres*, Vol. II, pp. 254–255.

In the second theorem above we have said nothing concerning the character of the integer k except that it is positive. We shall now show that it is greater than 1, whence it will follow that z is divisible by p^2. From formulæ (9) we have

$$u_2{}^p + u_3{}^p = x + y + 2z \equiv 0 \bmod p.$$

From this it follows that $u_2 + u_3$ is divisible by p. Let us write

$$u_2 = -u_3 + p\alpha.$$

Then

$$u_2{}^p \equiv -u_3{}^p \bmod p^2 \quad \text{or} \quad u_2{}^p + u_3{}^p \equiv 0 \bmod p^2.$$

Thence, by aid of the last formula in (10), we see that z is divisible by p^2, and hence that $k > 1$.

We shall show next that the prime factors of v_1 in both theorems are of the form $2hp^2+1$, where h is a positive integer. Let q be a prime factor of v_1. Then in either case we have

$$v_1 \equiv 0, \quad z \equiv 0, \quad y \equiv u_2{}^p, \quad x \equiv u_3{}^p, \quad x^p + y^p \equiv u_2{}^{p^2} + u_3{}^{p^2} \equiv 0 \bmod q \quad (11)$$

Let α be an integer such that $u_3\alpha \equiv 1 \bmod q$. Then the last congruence in (11) gives rise to the following:

$$(u_2\alpha)^{p^2} + 1 \equiv 0 \bmod q.$$

From this relation we see that

$$(u_{2\alpha})^{2p^2} \equiv 1, \quad u_{2\alpha} \not\equiv 1, \quad (u_{2\alpha})^{p} \not\equiv 1 \bmod q. \tag{12}$$

Let m be the exponent to which $u_{2\alpha}$ belongs modulo q. (See Carmichael, *l. c.*, pp. 61–63.) From relations (12) it follows that m is a divisor of $2p^2$, but is different from 1 and p. Hence m must have one of the values, 2, $2p$, p^2, $2p^2$. We shall show that it cannot have the value 2 or the value $2p$, and hence that $m = p^2$ or $m = 2p^2$.

Suppose that $m = 2$. Then $u_{2\alpha} \equiv -1 \bmod q$. This, together with the relation $u_{3\alpha} \equiv 1 \bmod q$, yields the congruence $u_2 + u_3 \equiv 0 \bmod q$; whence $x + y \equiv 0 \bmod q$. But this is impossible, since v_1 is prime to $x+y$ and q is a factor of v_1. Hence $m \neq 2$.

Next suppose that $m = 2p$. Then, in view of the last relation in (12), we see that $(u_{2\alpha})^{p} \equiv -1 \bmod q$. But $(u_{3\alpha})^{p} \equiv 1 \bmod q$. Hence $u_2^{p} + u_3^{p} \equiv 0 \bmod q$; whence $x + y \equiv 0 \bmod q$. Since the last relation is impossible, it follows that $m \neq 2p$.

Then $m = p^2$ or $m = 2p^2$. In either case $q - 1$ is divisible by p^2, and hence by $2p^2$ since q obviously is odd. Therefore q is of the form $2hp^2 + 1$, as was to be proved.

In the case of theorem I we see by symmetry that the prime factors of v_2 and v_3 are also of the form $2hp^2 + 1$.

In the case of theorem II it may be shown similarly that the prime factors of v_2 and v_3 are of the form $2hp + 1$. It is sufficient to treat one of the numbers, say v_2. Then we have

$$y^{p} + z^{p} \equiv 0 \bmod q,$$

where q is a prime factor of v_2 and is hence prime to y and z. This relation may be treated in the same manner as the last relation in (11) was treated above, and with the result already stated. The reader can readily supply the argument.

Among the methods which conceivably might be used separately for the proof of the Fermat theorem are the following: Assume that Eq. (2) is satisfied and find a set of contradictory properties of x, y, z; assume that Eq. (2) is satisfied and find a set of contradictory properties of p. (These two methods might clearly be included in the more general one in which contradictory properties of x, y, z, p would be

obtained.) Theorems I and II above give properties of x, y, z; they may be thought of in connection with the first method of proof just mentioned. We shall now derive some properties of p which are necessary if (2) is to be satisfied; the results so obtained may be thought of in connection with the second method of proof just mentioned.

Let us suppose that Eq. (2) has solutions in integers x, y, z which are prime to each other and to p. Let q be a prime number of the form $2hp+1$. Suppose first that q is not a factor of any one of the numbers x, y, z. Then from Eq. (2) we have

$$x^p+y^p+z^p\equiv 0 \bmod q. \tag{13}$$

Let z_1 be a number such that $zz_1\equiv 1 \bmod q$. Then we have

$$(xz_1)^p+1\equiv(-yz_1)^p \bmod q,$$

a relation which we shall write in the form

$$s^p+1\equiv t^p \bmod q. \tag{14}$$

Raising each member of this congruence to the $2h$th power and simplifying by means of the relations

$$s^{2hp}\equiv 1, \quad t^{2hp}\equiv 1 \bmod q, \tag{15}$$

we have

$$\binom{2h}{1}s^{(2h-1)p}+\binom{2h}{2}s^{(2h-2)p}+\cdots+\binom{2h}{2h-1}s^p+1\equiv 0 \bmod q, \tag{16a}$$

the parentheses quantities being binomial coefficients. Multiplying this congruence through repeatedly by s^p and simplifying by means of the first relation in (15), we have

$$\left.\begin{aligned}
&\binom{2h}{2}s^{(2h-1)p}+\binom{2h}{3}s^{(2h-2)p}+\cdots+1\cdot s^p+\binom{2h}{1}\equiv 0 \bmod q,\\
&\binom{2h}{3}s^{(2h-1)p}+\binom{2h}{4}s^{(2h-2)p}+\cdots+\binom{2h}{1}s^p+\binom{2h}{2}\equiv 0 \bmod q,\\
&\qquad\cdots\qquad\cdots\qquad\cdots\qquad\cdots\qquad\cdots\qquad\cdots\qquad\cdots\\
&1\cdot s^{(2h-1)p}+\binom{2h}{1}s^{(2h-2)p}+\cdots+\binom{2h}{2h-2}s^p+\binom{2h}{2h-1}\equiv 0 \bmod q
\end{aligned}\right\} \tag{16b}$$

It is clear that the existence of congruences (16) implies that

$$D_{2h}\equiv 0 \bmod q, \tag{17}$$

where D_{2h} denotes the determinant

$$D_{2h}=\begin{vmatrix} \binom{2h}{1} & \binom{2h}{2} & \cdots & \binom{2h}{2h-1} & 1 \\ \binom{2h}{2} & \binom{2h}{3} & \cdots & 1 & \binom{2h}{1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \binom{2h}{1} & \cdots & \binom{2h}{2h-2} & \binom{2h}{2h-1} \end{vmatrix}$$

We may look on (14) and (17) as giving necessary properties of q when no one of the numbers x, y, z is divisible by q.

Let us next suppose that q is a factor of one of the numbers x, y, z; say that it is a factor of z. Then from Eq. (8) we have

$$(-u_1)^p+u_2{}^p+u_3{}^p\equiv 0 \bmod q. \tag{18}$$

Now, q is a factor of u_1 or of v_1, since it is a factor of z. Suppose that q is a factor of v_1. Then it is not a factor of $-u_1$, u_2, or u_3. Therefore congruence (18) may be used just as (13) was employed above to derive a necessary relation of the form (14) and thence the necessary relation (17). Suppose next that q is a factor of u_1. Then (18) becomes

$$u_2{}^p+u_3{}^p\equiv 0 \bmod q;$$

whence

$$u_2{}^{2p}\equiv u_3{}^{2p} \bmod q. \tag{19}$$

Now, by means of Eqs. (2) and (8) and the polynomial theorem we see that

$$\begin{aligned}(u_1{}^p+u_2{}^p+u_3{}^p)^p &= (u_1{}^p+u_2{}^p+u_3{}^p)^p-(u_1{}^p+u_2{}^p-u_3{}^p)^p \\ &\quad -(u_1{}^p-u_2{}^p+u_3{}^p)^p-(-u_1{}^p+u_2{}^p+u_3{}^p)^p \\ &= \sum \frac{p!}{\alpha!\beta!\gamma!}u_1{}^{\alpha p}u_2{}^{\beta p}u_3{}^{\gamma p}(1-(-1)^\alpha-(-1)^\beta-(-1)^\gamma), \end{aligned} \tag{20}$$

where the summation is taken over all non-negative numbers α, β, γ for which $\alpha+\beta+\gamma=p$. Of the numbers α, β, γ in a given set, either one is odd or three are odd, since their sum is the odd number p. For a set in which only one of them is odd

the parenthesis expression in (20) vanishes. Hence from (20) we have the relation

$$(u_1^p+u_2^p+u_3^p)^p$$
$$=4pu_1^pu_2^pu_3^p\sum\frac{(p-1)!}{(2\lambda+1)!(2\mu+1)!(2\nu+1)!}u_1^{2\lambda p}u_2^{2\mu p}u_3^{2\nu p}, \quad (21)$$

where the summation is taken over all non-negative numbers λ, μ, ν for which $\lambda+\mu+\nu=\frac{1}{2}(p-3)$. Hence we may write

$$u_1^p+u_2^p+u_3^p=2pu_1u_2u_3P,$$

$$\sum\frac{(p-1)!}{(2\lambda+1)!(2\mu+1)!(2\nu+1)!}u_1^{2\lambda p}u_2^{2\mu p}u_3^{2\nu p}=2^{p-2}p^{p-1}P^p. \quad (22)$$

For the case under consideration u_1 is a multiple of q while from (19) we see that

$$u_2^{2\mu p}u_3^{2\nu p}\equiv u_2^{2(\mu+\nu)p} \bmod q.$$

Hence from (22) we have

$$u_2^{(p-3)p}\sum\frac{(p-1)!}{(2\mu+1)!(2\nu+1)!}\equiv 2^{p-2}p^{p-1}P^p \bmod q,$$

since q is a factor of every term in the first member of (21) for which $\lambda\neq 0$. Here the summation is for all non-negative values of μ and ν for which $\mu+\nu=\frac{1}{2}(p-3)$. Now the sum indicated by Σ in the last congruence has the value 2^{p-2}, as one sees readily by expanding $(1+1)^{p-1}$ and $(1-1)^{p-1}$ by the binomial theorem and taking half their difference. Hence

$$u_2^{(p-3)p}\equiv p^{p-1}P^p \bmod q.$$

From this it follows that P is not divisible by q. Moreover, taking the $2h$th power of each member of the last congruence we have

$$1\equiv p^{2h(p-1)} \bmod q;$$

or,

$$p^{2h}\equiv 1 \bmod q.$$

This is a necessary condition on q in the case now under consideration.

Gathering together the last result and those associated with relations (14) and (17) we have the following theorem:

III. *If p is an odd prime number having the property that a prime number q exists, $q=2hp+1$, such that $p^{2h}-1$ is not divisible by q and either*

$$D_{2h} \not\equiv 0 \bmod q,$$

where D_{2h} denotes the determinant introduced in Eq. (17), or the congruence

$$s^p+1 \equiv t^p \bmod q,$$

has no solution in integers s and t which are prime to q; then the equation $x^p+y^p+z^p=0$ cannot be satisfied by integers x, y, z, which are prime to p.

Next let us suppose that Eq. (2) has a solution in integers x, y, z which are prime each to each, one of them being divisible by p. We shall suppose that it is z which is divisible by p. In this case we shall need to employ the relations in theorem II. Replacing Eq. (21), we shall now have another, obtained in a similar manner; namely:

$$(p^{kp-1}u_1{}^p+u_2{}^p+u_3{}^p)^p$$

$$=4p^{kp}u_1{}^pu_2{}^pu_3{}^p\sum\frac{(p-1)!}{(2\lambda+1)!(2\mu+1)!(2\nu+1)!}p^{2\lambda(kp-1)}u_1{}^{2\lambda p}u_2{}^{2\mu p}u_3{}^{2\nu p};$$

whence we may write

$$p^{kp-1}u_1{}^p+u_2{}^p+u_3{}^p=2p^ku_1u_2u_3\cdot P,$$

$$\sum\frac{(p-1)!}{(2\lambda+1)!(2\mu+1)!(2\nu+1)!}p^{2\lambda(kp-1)}\cdot u_1{}^{2\lambda p}u_2{}^{2\mu p}u_3{}^{2\nu p}=2^{p-2}P^p. \quad (23)$$

We shall presently have need for the last relation.

Again, let q be a prime number of the form $2hp+1$. If we suppose that q is not a factor of any one of the numbers x, y, z, we shall be led as before to relations (14) and (17). We shall therefore direct our attention to the other case, namely, that in which q is a factor of one of the numbers x, y, z.

Suppose that q is a factor of x. Then from (10) we have

$$p^{kp-1}u_1{}^p-u_2{}^p+u_3{}^p\equiv 0 \bmod q. \quad (24)$$

Now, q is a factor of u_2 or of v_2, since it is a factor of x. First suppose that it is a factor of v_2. Then it is prime to u_1, u_2, u_3. Let u be chosen so that $p^{k-1}u_1u\equiv 1 \bmod q$ and multi-

ply both members of congruence (24) by u^p. A relation is obtained which may be written in the form

$$p^{p-1} \equiv s^p + t^p \bmod q, \tag{25}$$

where s and t are prime to q. This congruence may now be employed in the way in which (14) was used in the preceding argument. A set of congruences modulo q, $2h$ in number, may be found in the following manner: The first arises from (25) by raising each member to the $2h$th power and simplifying by means of relations (15). The others come from this one by repeated multiplication by $s^p t^{(2h-1)p}$ and reduction by means of (15). The existence of these $2h$ congruences implies that

$$\Delta_{2h} \equiv 0 \bmod q, \tag{26}$$

where

$$\Delta_{2h} = \begin{vmatrix} \binom{2h}{1} & \binom{2h}{2} & \cdots & \binom{2h}{2h-1} & 2 - p^{2h(p-1)} \\ \binom{2h}{2} & \binom{2h}{3} & \cdots & 2 - p^{2h(p-1)} & \binom{2h}{1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 2 - p^{2h(p-1)} & \binom{2h}{1} & \cdots & \binom{2h}{2h-2} & \binom{2h}{2h-1} \end{vmatrix}.$$

Next let us suppose that q is a factor of u_2. Then from (24) we have readily

$$u_3^{2p} \equiv p^{2(kp-1)} u_1^{2p} \bmod q.$$

Employing (23) now as we did (22) in the previous case, we have

$$p^{(p-3)(kp-1)} u_1^{p(p-3)} \equiv P^p \bmod q. \tag{27}$$

Raising each member of this congruence to the $2h$th power and simplifying, we have

$$p^{6h} \equiv 1 \bmod q.$$

This, in connection with the relation $p^{2hp} \equiv 1 \bmod q$, leads to the congruence

$$p^{2h} \equiv 1 \bmod q,$$

provided that p is greater than 3.

It is obvious that in the case in which q is a factor of y, we should be led to the same relations as those just obtained when q is a factor of x.

Finally, let us suppose that q is a factor of z. Then from (10) we have

$$-p^{kp-1}u_1{}^p+u_2{}^p+u_3{}^p\equiv 0 \bmod q.$$

Now, q is a factor of u_1 or of v_1, since it is a factor of z. If we suppose that q is a factor of v_1, we shall be led as before to relation (26). If we suppose that q is a factor of u_1, then from (9) we have $x+y\equiv 0 \bmod q$.

Gathering together the results just deduced and those in theorem III, we have the following theorem:

IV. *If there exists a prime number* q, $q=2hp+1$, *which is not a factor of any of the numbers*

$$D_{2h},\quad \Delta_{2h},\quad p^{2h}-1,$$

and if the equation

$$x^p+y^p+z^p=0$$

is satisfied by integers x, y, z, *which are prime each to each, then one of these integers (say* z*) and the sum of the other two (say* $x+y$*) are both divisible by* q.

We shall give one other theorem which may be demonstrated by elementary means; namely, the following:

V. *If* p *is an odd prime and the equation*

$$x^p+y^p+z^p=0, \qquad (2^{\text{bis}})$$

has a solution in integers x, y, z, *each of which is prime to* p, *then there exists a positive integer* s, *less than* $\frac{1}{2}(p-1)$, *such that*

$$(s+1)^p\equiv s^p+1 \bmod p^3. \qquad (28)$$

From Eq. (7) we have

$$(x+y)^{p-1}\equiv u_1{}^{p(p-1)}\equiv 1 \bmod p^2.$$

This relation and two similar ones lead to the following:

$$(x+y)^p\equiv x+y,\quad (y+z)^p\equiv y+z,\quad (z+x)^p\equiv z+x \bmod p^2. \qquad (29)$$

Now,

$$x+y\equiv -z \bmod p;$$

whence

$$(x+y)^p\equiv -z^p\equiv x^p+y^p \bmod p^2. \qquad (30)$$

Similarly,

$$(y+z)^p \equiv y^p+z^p, \quad (z+x)^p \equiv z^p+x^p \bmod p^2. \tag{31}$$

From relations (29), (30), (31) and Eq. (2^{bis}), we have

$$x+y+z \equiv 0 \bmod p^2.$$

From this we have

$$(x+y)^p \equiv -z^p \equiv x^p+y^p \bmod p^3.$$

Let u be an integer such that $yu \equiv 1 \bmod p^3$. Then we have

$$(xu+1)^p \equiv (xu)^p+1 \bmod p^3.$$

Hence we have the congruence

$$(\sigma+1)^p \equiv \sigma^p+1 \bmod p^3, \tag{32}$$

where σ is a positive integer less than p^3.

We shall next show that congruence (32) implies and is implied by the congruence

$$(\sigma+1)^{p^2} \equiv \sigma^{p^2}+1 \bmod p^3. \tag{33}$$

Let us define integers λ and μ by means of the relations

$$(\sigma+1)^p = \sigma+1+\lambda p, \quad \sigma^p = \sigma+\mu p.$$

Then

$$(\sigma+1)^p = \sigma^p+1+(\lambda-\mu)p. \tag{34}$$

We have also

$$(\sigma+1)^{p^2} \equiv (\sigma+1)^p+\lambda p^2(\sigma+1)^{p-1} \bmod p^3,$$

$$\equiv \sigma+1+\lambda p+\lambda p^2 \bmod p^3.$$

Likewise

$$\sigma^{p^2} \equiv \sigma+\mu p+\mu p^2 \bmod p^3.$$

From the last two congruences we have

$$(\sigma+1)^{p^2} \equiv \sigma^{p^2}+1+(\lambda-\mu)(p+p^2) \bmod p^3. \tag{35}$$

From (34) and (35) we see that a necessary and sufficient condition for either (32) or (33) is that $\lambda-\mu \equiv 0 \bmod p^2$. Therefore, (32) and (33) are equivalent; that is, if one of these congruences is satisfied for a given value of σ, so is the other.

In view of this result we shall have proved relation (28) as soon as we have shown the existence of an integer s less than $\frac{1}{2}(p-1)$ and such that

$$(s+1)^{p^2} \equiv s^{p^2}+1 \bmod p^3. \tag{36}$$

Let t be that residue of σ modulo p for which the absolute value is a minimum. Then from (33) we have

$$(t+1)^{p^2} \equiv t^{p^2}+1 \bmod p^3.$$

Three cases are possible. (*a*) We may have $t=\frac{1}{2}(p-1)$. Then

$$(p+1)^{p^2} \equiv (p-1)^{p^2}+2^{p^2} \bmod p^3$$

or

$$2^{p^2} \equiv 1^p+1 \bmod p^3,$$

so that for this case we may take $s=1$. (*b*) We may have t positive and less than $(\frac{1}{2}(p-1)$. In this case we may take $s=t$. (*c*) We may have t negative and greater than $-\frac{1}{2}(p-1)$. In this case we write $s+1=-t$; then

$$(-s)^{p^2} \equiv (-s-1)^{p^2}+1 \bmod p^3;$$

whence (36) follows readily and then (28).

This completes the proof of the theorem.

By means of theorem III, Legendre has shown that the equation $x^p+y^p+z^p=0$ cannot be satisfied by integers x, y, z, each of which is prime to p if $p<197$. Maillet has shown that the same is true if $p<223$. Mirimanoff has extended the result to every p less than 257. By a further penetrating discussion Dickson (*Quart. Journ. Math.*, vol. 40) has proved that the equation is without a solution in integers prime to p if $p<6857$.

We shall illustrate the means of obtaining these results by proving that *the equation* $x^p+y^p+z^p=0$ *has no solution in integers* x, y, z, *prime to* p *if* $2p+1$ *or* $4p+1$ *is a prime.* For this purpose we employ theorem III.

If $2p+1$ is a prime, we may take $q=2p+1$ and $h=1$. Then

$$D_2=\begin{vmatrix} 2 & 1 \\ 1 & 2 \end{vmatrix}=3.$$

Now $2p+1$ is not a factor either of 3 or of $p^2-1=(p-1)(p+1)$. If $4p+1$ is a prime, we may take $h=2$. Then

$$D_4=\begin{vmatrix} 4 & 6 & 4 & 1 \\ 6 & 4 & 1 & 4 \\ 4 & 1 & 4 & 6 \\ 1 & 4 & 6 & 4 \end{vmatrix}=-3\cdot 5^3.$$

Now $4p+1$ is not a factor of 3.5^3 or of

$$p^4-1=(p-1)(p+1)(p^2+1).$$

From these results and theorem III, we conclude that the equation $x^p+y^p+z^p=0$ has no solution in integers x, y, z, prime to p if either $2p+1$ or $4p+1$ is a prime; in particular, therefore, if

$$p=3,\ 5,\ 7,\ 11,\ 13,\ 23,\ 29,\ 41,\ \ldots$$

§ 22. Present State of Knowledge Concerning the Equation $x^p+y^p+z^p=0$

In the present section we shall give a brief statement of the more important known facts about the equation

$$x^p+y^p+z^p=0, \quad p=\text{odd prime}, \tag{1}$$

over and above those which we have already mentioned. These have not yet been demonstrated by elementary means; and therefore a proof of them would be out of place in this introductory book.

Cauchy (*Comptes Rendus* of Paris, Vol. XXV, p. 181; *Œuvres*, (1) 10: 364) states without proof the remarkable theorem that if Eq. (1) is satisfied by integers x, y, z which are prime to p, then

$$1^{p-4}+2^{p-4}+3^{p-4}+\ldots+\{\tfrac{1}{2}(p-1)\}^{p-4}\equiv 0 \bmod p.$$

It is to Kummer that we owe the most important development of the theory of Eq. (1). (See references to Kummer's work in H. J. S. Smith's Report on the Theory of Numbers in Smith's *Collected Mathematical Papers*, Vol. I, p. 97.) Kummer makes use of complex numbers and by aid of them proves the following general theorem:

If p is a prime number which is not a factor of the numerator of one of the first $\frac{1}{2}(p-3)$ Bernoulli numbers, then Eq. (1) has no solution in integers x, y, z, all of which are different from zero.

In case p is a factor of one of the first $\frac{1}{2}(p-3)$ Bernoulli numerators, Kummer finds other properties which it must possess. These we shall not state.

By means of his general theorem Kummer shows in particular that Eq. (1) is impossible if $p \leqq 100$.

Starting from results due to Kummer, Wieferich (Crelle's Journal, Vol. CXXXVI) has shown that if Eq. (1) is satisfied by integers prime to p then *

$$2^{p-1} \equiv 1 \bmod p^2.$$

Mirimanoff (Crelle's Journal, Vol. CXXXIX) has shown that p must in this case also satisfy the relation

$$3^{p-1} \equiv 1 \bmod p^2.$$

He also derives other relations which are less simple in form.

Later Furtwängler has proved two theorems from which the above criteria of Wieferich and Mirimanoff may be deduced. These theorems are as follows:

If x_1, x_2, x_3 are three integers, different from zero and without common divisor, among which subsists the equation

$$x_1^p + x_2^p + x_3^p = 0,$$

where p is an odd prime, then

I. Every factor r of x_i $(i = 1, 2, 3)$ satisfies the congruence

$$r^{p-1} \equiv 1 \bmod p^2,$$

if x_i is prime to p;

II. Every factor r of $x_i \pm x_k$ $(i, k = 1, 2, 3)$ satisfies the congruence

$$r^{p-1} \equiv 1 \bmod p^2,$$

if $x_i + x_k$ and $x_i - x_k$ are prime to p.

By means of relations due to Mirimanoff and Furtwängler, Vandiver (Trans. Amer. Math. Soc., Vol. XV) has shown that if Eq. (1) has a solution in integers x, y, z, all of which are prime to p, then p has the following property:

(1) If p is of the form $3n+1$, then either

$$2^{p-1} \equiv 1 \bmod p^4 \quad \text{or} \quad 5^{p-1} \equiv 1 \bmod p^2;$$

(2) If p is of the form $3n+2$, then either

$$2^{p-1} \equiv 1 \bmod p^4 \quad \text{or} \quad 5^{p-1} \equiv 7^{p-1} \equiv 1 \bmod p^2.$$

* The smallest prime p for which this relation is satisfied is $p = 1093$. There is no other p less than 2000 satisfying this relation.

Vandiver has also recently announced (Bull. Amer. Math. Soc., March, 1915) that he has found a relation which implies several of those previously obtained, in particular, those in the theorems of Furtwängler above.

Reference should also be made to two papers by Bernstein, one by Furtwängler, and one by Hecke in the *Göttinger Nachrichten* for 1910.

In conclusion it is to be remarked that the Academy of Sciences of Göttingen holds a sum of 100,000 marks which is to be awarded as a prize to the person who first presents a rigorous proof of Fermat's Last Theorem. The existence of this prize money has called forth a large number of pseudo-solutions of the problem. Unfortunately, the number of untrained workers attacking the problem seems to be increasing.

GENERAL EXERCISES

1.* There do not exist three binary forms which afford a solution of the equation $x^n+y^n=z^n$, $n>2$, for every pair of values of the variables in those forms. (Carlini, 1911.)

2. If the equation $x^n+y^n=z^n$ is impossible, so is each of the equations $u^{2n}-4v^n=t^2$ and $s(2s+1)=t^{2n}$. (Lind, 1910.)

3. If the equation $x^n+y^n=z^n$ is impossible, so is each of the equations $u^{2n}+v^{2n}=t^2$ and $u^{2n}-v^{2n}=2t^n$. (Liouville, 1840.)

4. If the equation $x^k+y^k=z^k$ is impossible for every k greater than 2, then is the equation $u^mv^n+v^mw^n+w^mu^n=0$ impossible for every pair of integers m and n, except for the trivial solutions 1, 0, 0; 0, 1, 0; 0, 0, 1. (Hurwitz, 1908.)

5.† Determine systematically a large number of simple equations which are impossible when $x^n+y^n=z^n$ has no solution.

6.* If we write

$$s_1=x+y+z, \quad s_2=xy+yz+zx, \quad s_3=xyz,$$

then the condition

$$x^p+y^p+z^p=0, \tag{1}$$

can be written in the form

$$\phi_p(s_1, s_2, s_3)=0, \tag{2}$$

while x, y, z are roots of the cubic equation

$$t^3-s_1t^2+s_2t-s_3=0. \tag{3}$$

Then Eq. (1) can have a rational solution only when all the roots of (3) are rational, its coefficients being subject to the condition (2). By aid of this remark show that (1) is impossible when $p=17$. (Mirimanoff, 1909.)

7.* If the equation $x^p+y^p+z^p=0$ has the primitive solution x, y, z, p being an odd prime, and G is the greatest common divisor of $x+y+z$ and x^2+xy+y^2, then integers I, K, L exist such that

$$y^2+yz+z^2=GI, \quad z^2+zx+x^2=GK, \quad x^2+xy+y^2=GL,$$

and all the factors of the numbers I, K, L are of the form $6\mu p+1$. Show that to demonstrate the impossibility of the equation $x^p+y^p+z^p=0$ it is sufficient to prove that two of the numbers I, K, L are equal or that one of them is unity. (Fleck, 1909.)

8. Show that the equation $3u(4v^3-u^3)=t^2$ is impossible in integers u, v, t, all of which are different from zero.

9.† Note that when p is an odd prime the equation

$$x^{2p}+y^{2p}=z^{2p},$$

with the condition that x, y, z are prime to p, implies the three Pythagorean equations

$$x^2+y^2=z_1^2, \quad x_1^2+y^2=z^2, \quad x^2+y_1^2=z^2.$$

What numbers x, y, z can satisfy these three equations?

10. Show that the equation $x^{2p}+y^{2p}=z^{2p}$, in which p is a prime number, implies the coexistence of two equations of the form

$$a^p+b^p=c^p, \quad b^p+c^p=d^p.$$

11.* Investigate the problem of solving the equation $x^p+y^p=pz^p$, where p is an odd prime. (Hayashi, 1911.)

12.* Investigate the problem of solving the equation $x^p+y^p=cz^p$, where p is an odd prime. (Maillet, 1901.)

13.* Prove that neither of the equations $t^2=(z^2+y^2)^2-(zy)^2$, $t^2=(z^2-y^2)^2-(zy)^2$ possesses an integral solution. By means of this result prove the impossibility of each of the equations

$$u^6+v^6=w^6, \quad u^{10}+v^{10}=w^{10}. \qquad \text{(Kapferer, 1913.)}$$

CHAPTER VI

THE METHOD OF FUNCTIONAL EQUATIONS

§ 23. Introduction. Rational Solutions of a Certain Functional Equation

There is a method which will sometimes be found useful in the theory of Diophantine analysis and which we have had no occasion to employ in the preceding pages. It may conveniently be described as the method of functional equations. It consists essentially in the use of rational solutions of functional equations as an aid in solving Diophantine problems of a certain type, a type in fact which plays an important role in the work of Diophantus. In this chapter we shall give a brief illustration of the method by employing it in the solution of certain problems first treated by Diophantus and Fermat.

It should be said that the principal value of this method lies not so much in its use for the solution of given problems as in the fact that it renders possible an arrangement of certain problems in an order in which they may profitably be investigated. A treatment of these problems from this point of view seems not to exist in the literature. The primary purpose of this chapter is to direct attention to the possibilities of this general method of functional equations and to give an indication of how it may be employed. A general systematic development of the method is not attempted.

Diophantus more than once makes use of the identity

$$a^2(a+1)^2+a^2+(a+1)^2=(a^2+a+1)^2$$

in the solution of problems. This identity may be looked upon as affording a solution of the functional equation

$$a^2u_a^2+a^2+u_a^2=v_a^2, \tag{1}$$

in which u_a and v_a are to be determined as rational functions of a. It is clear that this equation may be written in the form

$$(a^2+1)(u_a^2+1)=v_a^2+1. \tag{2}$$

The first member may be written as a sum of two squares, thus

$$(a^2+1)(u_a^2+1)=(au_a\pm 1)^2+(u_a\mp a)^2. \tag{3}$$

The second member may be written as a sum of two squares in a great variety of ways. Thus, if we write

$$v_a^2+1=(v_a+x_a)^2+(1+m_ax_a)^2, \tag{4}$$

we have

$$2v_ax_a+x_a^2+2m_ax_a+m_a^2x_a^2=0.$$

Besides the solution $x_a=0$ of this equation, we have

$$x_a=-\frac{2(m_a+v_a)}{m_a^2+1}.$$

Thence we see that

$$v_a^2+1=\left\{v_a-\frac{2(m_a+v_a)}{m_a^2+1}\right\}^2+\left\{1-\frac{2m_a(m_a+v_a)}{m_a^2+1}\right\}^2. \tag{5}$$

From (3) and (5) we see that (2) will be satisfied if

$$\left.\begin{aligned} au_a\pm 1&=v_a-\frac{2(m_a+v_a)}{m_a^2+1},\\ u_a\mp a&=1-\frac{2m_a(m_a+v_a)}{m_a^2+1}.\end{aligned}\right\} \tag{6}$$

It is obvious that these two equations may be solved rationally for u_a and v_a in terms of m_a, so that we have a rational solution of (2), and hence of (1), for every rational function m_a. This solution may be written in the following form:

$$\left.\begin{aligned} u_a&=\pm a-1+\frac{2}{m_a^2+1}-\frac{2m_a}{m_a^2+1}\left\{-a\pm\frac{(a^2+1)(m_a\pm 1)^2}{m_a^2+2am_a-1}\right\},\\ v_a&=-a\pm\frac{(a^2+1)(m_a\pm 1)^2}{m_a^2+2am_a-1}.\end{aligned}\right\} \tag{7}$$

To the solution of (1) afforded by (7) we should adjoin those gotten by taking $x_a=0$ in (4), namely:

$$u_a=\pm a+1,\quad v_a=a\pm(a^2+1),\quad u_a=\frac{2}{a},\quad v_a=a+\frac{2}{a}.$$

We write down some simple particular solutions for which we shall have use in § 25.

$$\left.\begin{array}{llll} u_a = a+1, & \dfrac{2}{a}, & 2a^2, & \\ v_a = a^2+a+1, & a+\dfrac{2}{a}, & a(2a^2+1), & \\ u_a = 4a^3+4a^2+3a+1, & & & \\ v_a = 4a^4+4a^3+5a^2+3a+1. & & & \end{array}\right\} \tag{8}$$

§ 24. Solution of a Certain Problem from Diophantus

In Book V of his *Arithmetica* Diophantus proposes and shows how to solve the following problem:

To find three squares such that the product of any two of them, added to the sum of those two or to the remaining one, gives a square.

If we denote one of these squares by a^2 it will be convenient to take $u_a{}^2$ for a second one, where u_a is one of the functions denoted by this symbol in the preceding section. For this purpose Diophantus uses $u_a = a+1$. He then observes that the three numbers,

$$a^2, \quad (a+1)^2, \quad 4a^2+4a+4, \tag{1}$$

have the property that the product of any two of them, added to the sum of those two or to the remaining one, gives a square. This may readily be verified by the reader. Then to complete the solution of the problem it is sufficient to render $4a^2+4a+4$, and hence a^2+a+1, equal to a square. Setting, as usual,

$$a^2+a+1 = (m-a)^2,$$

we have

$$a = \frac{m^2-1}{2m+1}, \tag{2}$$

where m is any rational number whatever. If this value of a is set in expressions (1) we have the three squares sought.

Fermat has shown that this result * of Diophantus may be employed in the solution of the following problem:

* It may be remarked that the result of the next section may also be used for the same purpose.

To find four numbers such that the product of any two of them added to the sum of those two gives a square.

For three of the numbers sought take a set of numbers (1) where a has the form given in (2). Following Fermat, we shall take the particular set given by Diophantus, namely:

$$\frac{25}{9}, \quad \frac{64}{9}, \quad \frac{196}{9}.$$

This is obtained by taking $m=-2$ in equation (4). Let x be the fourth number sought. Then it is necessary and sufficient that x satisfy the conditions *

$$\frac{34}{9}x+\frac{25}{9}=\square, \quad \frac{73}{9}x+\frac{64}{9}=\square, \quad \frac{205}{9}x+\frac{196}{9}=\square;$$

or more simply the conditions

$$34x+25=\square, \quad 73x+64=\square, \quad 205x+196=\square. \tag{3}$$

This is an example of the so-called *triple equation* of Fermat. We shall find a solution by the method originated by Fermat. Replace x by a function of t in such way that the first equation in (3) shall be satisfied. For this purpose it is sufficient to take

$$x=34t^2+10t.$$

Then the other two equations in (3) become

$$2482t^2+730t+64=\square, \quad 14{,}965t^2+2050t+196=\square. \tag{4}$$

We have to determine t so as to satisfy these equations, an example of the so-called *double equation* of Fermat.

The interesting method of Fermat enables one to find an indefinitely great number of solutions of system (4). Multiplying the first equation through by 196 and the second by 64, we have two new equations of the same form as (4) with the further condition that the independent terms in the first members are equal. These equations are

$$\left.\begin{aligned} 486{,}472t^2+143{,}080t+12{,}544=\square, \\ 957{,}760t^2+131{,}200t+12{,}544=\square, \end{aligned}\right\} \tag{5}$$

* The symbol $\square$ stands for a square number with whose value we are not concerned. It may differ from one equation to another.

The difference of the two first members is $471{,}288t^2 - 11{,}880t$. We may separate this into two factors, thus:

$$\frac{1425}{28}t \cdot \left(\frac{4{,}398{,}688}{475}t - 224\right). \tag{6}$$

The separation is effected in such way that the independent term in the second factor is twice the square root of the independent term 12,544 in Eqs. (5). Now, if half the sum of the two factors in (6) is squared and the result equated to the first member of the second equation in (5), it is obvious that a rational value of t will be obtained satisfying that equation. It is clear that this value will then also satisfy the other equation in (5). This value of t affords a value of x, the fourth number in the set to be determined.

Eqs. (4) have not merely a single solution, but an infinite number. These may be found one after the other as follows: Let t_1 be a value of t satisfying Eqs. (4) and write $t = u + t_1$. Putting this value of t in (4), we obtain a pair of equations in u of the same form as (4). These can be solved by the method just given for solving (4). We thus obtain a single solution $u = u_1$ of these equations. Then $t = u_1 + t_1$ is a solution of (4). By the aid of this solution of (4) another may be obtained; and so on indefinitely.

By means of each solution of (4) we obtain a new value of x affording a solution of the problem proposed.

It should be observed that the method of solving Eqs. (4), and hence that of solving Eqs. (3), is general, being applicable to all equations of the types (3) and (4).

§ 25. Solution of a Certain Problem Due to Fermat

Fermat has given attention to the following problem:

To find three squares such that the product of any two of them, added to the sum of those two, gives a square.

He has indicated that this problem is capable of a solution different from that which is incidental to the solution given by Diophantus for the first problem treated in the pre-

ceding section; but he gives no hint as to the method which he employs. He says, however, that it leads to an indefinitely great number of solutions. Making use of the solutions of the functional equation treated in § 23, we shall now give two methods for solving this problem with such result.

Let u_a and w_a be two rational functions of the rational number a such that

$$\left.\begin{aligned} a^2u_a^2+a^2+u_a^2 &= \square, \\ a^2w_a^2+a^2+w_a^2 &= \square. \end{aligned}\right\}, \tag{1}$$

Then if we take a^2, u_a^2, w_a^2 for the three squares sought, we have to determine a so as to satisfy the single equation

$$u_a^2w_a^2+u_a^2+w_a^2=\square. \tag{2}$$

For determining appropriate functions u_a and w_a we have the results of § 23.

Let us take

$$u_a=a+1, \quad w_a=\frac{2}{a}.$$

Then (2) becomes

$$(a+1)^2\left(\frac{2}{a}\right)^2+(a+1)^2+\left(\frac{2}{a}\right)^2=\square,$$

or

$$a^4+2a^3+5a^2+8a+8=\square.$$

By means of the general method of § 17 in Chapter IV, it is possible to find an infinite number of values of a satisfying this equation. For every such value of a the three numbers a^2, $(a+1)^2$, $4/a^2$ furnish a solution of our problem.

We may also proceed as follows: Denoting the square in the second member of (2) by t_a^2, we may write that equation in the form

$$(u_a^2+1)(w_a^2+1)=t_a^2+1.$$

The second member may be separated into a sum of two squares as in Eq. (5) of § 23. Thus we have an equation of the form

$$(u_a^2+1)(w_a^2+1)=\left\{t_a-\frac{2(n_a+t_a)}{n_a^2+1}\right\}^2+\left\{1-\frac{2n_a(n_a+t_a)}{n_a^2+1}\right\}^2,$$

where n_a is an arbitrary rational function of a. This equation will be satisfied if

$$u_a w_a + 1 = t_a - \frac{2(n_a + t_a)}{n_a^2 + 1},$$

$$u_a - w_a = 1 - \frac{2n_a(n_a + t_a)}{n_a^2 + 1}.$$

These equations may be solved rationally for w_a and t_a in terms of n_a and u_a. Thus, we have for w_a the value

$$w_a = \frac{(u_a - 1)(n_a^4 - 1) + 2n_a(n_a^3 + n_a^2 + n_a + 1)}{(n_a^2 + 1)(n_a^2 - 2n_a u_a - 1)}. \tag{3}$$

With this value of w_a, Eq. (2) will be satisfied whatever rational functions u_a and n_a may be. If u_a is given any value such as those in Eqs. (7) and (8) of § 23, the first equation in (1) is satisfied. It is then sufficient to determine a so that the second equation in (1) is satisfied. Then for this value of a the squares a^2, u_a^2, w_a^2 furnish a solution of our problem.

As an illustration of this result let us take

$$u_a = a + 1, \quad n_a = 1.$$

Then

$$w_a = -\frac{2}{a+1},$$

so that the condition on a may be written

$$\frac{4a^2}{(a+1)^2} + a^2 + \frac{4}{(a+1)^2} = \square;$$

or

$$a^4 + 2a^3 + 5a^2 + 4 = \square.$$

An unlimited number of values of a may be found satisfying this equation (see § 17). We may get one of them by taking for the square in the second member the quantity

$$\left(2 + \frac{5}{4}a^2\right)^2,$$

and proceeding according to the methods of § 17 in Chapter IV. Thus, we have $a = 32/9$. Then our three squares are

$$\frac{1024}{81}, \quad \frac{1681}{81}, \quad \frac{324}{1681}.$$

GENERAL EXERCISES

1.† Determine all the polynomial solutions of the functional equation

$$a^2u_a^2+a^2+u_a^2=v_a^2.$$

Apply the result to the solution of a group of Diophantine problems.

2.† Investigate the problem of finding three squares such that the product of any two of them exceeds the sum of those two by a square.

3.† Obtain a solution of the system of equations

$$u_xv_x-1=\square, \quad v_xw_x-1=\square, \quad w_xu_x-1=\square,$$

in which u_x, v_x, w_x are unknown rational functions of x. Apply the result to the solution of problems in Diophantine analysis. (Cf. *Diophantus*, Book IV, Problem 24.)

Suggestion.—The given equations may be written in the form

$$u_xv_x=\rho_x^2+1, \quad v_xw_x=\sigma_x^2+1, \quad w_xu_x=\tau_x^2+1. \tag{1}$$

Then if equations of the form

$$u_x=a_x^2+b_x^2, \quad v_x=c_x^2+d_x^2, \quad w_x=e_x^2+f_x^2 \tag{2}$$

are assumed and substitution is made in system (1), certain of the functions introduced in Eq. (2) may be determined in terms of the others. A rational solution of the given system of equations is thus obtained. This process is also capable of generalization in accordance with the suggestion afforded by Eq. (5) of § 23.

4.† Treat the corresponding problems for the system of functional equations

$$u_xv_x+1=\square, \quad v_xw_x+1=\square, \quad w_xu_x+1=\square.$$

(Cf. *Diophantus*, Book IV, Problem 23.)

5.† Find rational functions u_x, v_x, w_x such that the continued product of their squares increased by the square of each one of them separately shall be the square of a rational function of x. Apply the result to problems in Diophantine analysis. (Cf. *Diophantus*, Book V, Problem 24.)

6.† Find rational functions u_x, v_x, w_x such that the continued product of their squares decreased by the square of each one of them separately shall be the square of a rational function of x. Apply the result to problems in Diophantine analysis. (Cf. *Diophantus*, Book V, Problem 25.)

MISCELLANEOUS EXERCISES

1. Show how to find four numbers such that if one takes the square of their sum *plus* or *minus* any one singly, then all the eight resulting numbers are squares. (Diophantus.)

2. Show how to find three numbers whose sum is a square, such that the sum of the square of each and the succeeding number is a square. (Diophantus.)

3. Show how to find two numbers such that their product *plus* or *minus* their sum is a cube. (Diophantus.)

4. Show how to find three numbers such that the square of any one of them *plus* or *minus* the sum of the three is a square. (Diophantus; Hart, 1876.)

5. Show how to find three numbers such that the product of any two of them *plus* or *minus* the sum of the three is a square. (Diophantus.)

6. Show how to find four numbers such that the product of each two of them increased by unity shall be the same square. (Diophantus; Lucas, 1880.)

7.* Show how to find five numbers such that the product of each two of them increased by unity shall be a square. (Euler, Legendre.)

8.* Obtain the general solution of the Diophantine system $y=x^2+(x+1)^2$, $y^2=z^2+(z+1)^2$. Generalize the results by treating also the system $y=x^2+t(x+\alpha)^2$, $y^2=z^2+t(z+\beta)^2$. (Jonquières, 1878.)

9.* Develop a theory of the Diophantine system $x=4y^2+1$, $x^2=z^2+(z+1)^2$. (Gerono, 1878.)

10. Obtain a single-parameter solution of the system $x^2+y^2-1=u^2$, $x^2-y^2-1=v^2$. (Arch. Math. Phys., 1854.)

11.* Obtain the general solution of the Diophantine equation

$$y^2=x(x+1)(2x+1). \qquad \text{(Pepin, 1879.)}$$

12. Apply the identity

$$(s^2-2st-t^2)^4+(2s+t)s^2t(2t+2s)^4=(s^4+t^4+10t^2s^2+4st^3+12s^3t)^2$$

to the resolution of certain Diophantine equations. (Desboves, 1878.)

13. Find all the integral solutions of the equation $(x+1)^y=x^{y+1}+1$. (Meyl, 1876.)

14. Develop methods for finding solutions of the Diophantine equation

$$2x^2y^2+1=x^2+y^2+z^2. \qquad \text{(Valroff, 1912.)}$$

15. Develop methods for obtaining solutions of the Diophantine system

$$x=u^2, \quad x+1=2v^2, \quad 2x+1=3w^2. \qquad \text{(Gerono, 1878.)}$$

16. Determine those Pythagorean triangles for each of which the sum of the area and either of the legs is a square. (Diophantus.*)

17. Determine those Pythagorean triangles for each of which the area exceeds either leg by a square. (Diophantus.*)

18. Determine those Pythagorean triangles for each of which the area exceeds the hypotenuse or one leg by a square. (Diophantus.*)

19. Determine those Pythagorean triangles for each of which the sum of the area and e ther the hypotenuse or one leg is a square. (Diophantus.*)

20 Determine those Pythagorean triangles for each of which the line bisecting an acute angle is rational. (Diophantus.*)

21. Determine those Pythagorean triangles for each of which the sum of the area and the hypotenuse is a square and the perimeter is a cube. (Diophantus.*)

22. Determine those Pythagorean triangles for each of which the sum of the area and the hypotenuse is a cube and the perimeter is a square. (Diophantus.*)

23. Determine those Pythagorean triangles for each of which the sum of the area and one side is a square and the perimeter is a cube. (Diophantus.*)

24. Determine those Pythagorean triangles for each of which the sum of the area and one side is a cube and the perimeter is a square. (Diophantus.*)

25. Determine those Pythagorean triangles for each of which the perimeter is a square and the area is a cube. (Diophantus.*)

26. Determine those Pythagorean triangles for each of which the perimeter is a cube and the sum of the perimeter and area is a square. (Diophantus.*)

27. Give a method of finding an infinite number of solutions of each of the equations $x^3+y^3=u^2+v^2$; $x^{2m+1}+y^{2m+1}=u^2+v^2$, $m>1$. (Aubry, Miot. 1912.)

28. If a Diophantine equation can be separated into two members each of which is homogeneous and the numbers representing the degrees of the two members are relatively prime, show how solutions may always be obtained in an easy manner. By means of special examples show that this method may often be used to obtain results which are not trivial in character.

29. Find three squares in arithmetical progression such that the square root of each of them is less than a square by unity. (Evans and Martin, 1873.)

30. Obtain all the integral solutions of the equation $x^y=y^x$.

31. Determine all the positive integral solutions of the equation

$$4x^3-y^3=3x^2yz^2. \qquad \text{(Swinden, 1912.)}$$

32. Show that the system $xy+x+y=a^2$, $xy-x-y=b^2$ is impossible in integers x, y, a, b all of which are different from zero. (Aubry, 1911.)

33.* Obtain the general rational solution of the system of equations

$$ax^2+b=u^2, \quad cx^2+d=t^2. \qquad \text{(Welmin, 1912.)}$$

34.* Show that the equation $u^m+v^n=w^k$ in which m, n, k are positive integers possesses an algebraic solution u, v, w each function of which is expressible as

* In the case of Problems 16 to 26 Diophantus shows merely how to find particular rational solutions. It is doubtless difficult to find general solutions of some of these problems; but particular solutions may be found without great difficulty.

a polynomial in the single variable t in each of the following cases and only in these:

(1) $u^m+v^2=w^2$,

(2) $u^2+v^2=w^k$,

(3) $u^3+v^3=w^2$,

(4) $u^4+v^3=w^2$,

(5) $u^4+v^2=w^3$,

(6) $u^5+v^3=w^2$. (Welmin, 1904.)

35.* Obtain all the solutions of the equation

$$m \arctan \frac{1}{x}+n \arctan \frac{1}{y}=k\frac{\pi}{4}$$

in integers k, m, n, x, y, showing that there are but the following four sets: 1, 1, 1, 2, 3; 1, 2, −1, 2, 7; 1, 2, 1, 3, 7; 1, 4, −1, 5, 239. (Störmer, 1899.)

36.* Develop the theory of the equation $ax^{p^t}+by^{p^t}=cz^{p^t}$, p being a prime number. (Maillet, 1898.)

37.* Develop the theory of the equation $ax^m+by^m=cz^n$. (Desboves, 1879.)

38. Of each of the following equations find a solution involving two or more parameters:

$$x^3+y^3+z^3=2t^3,$$

$$x^3+y^3+z^3=2t^{9k},$$

$$x^3+y^3+z^3+u^3=3t^3,$$

$$x^3+y^3+z^3+u^3=kt^m,$$

$$x^3+2y^3+3z^3=t^3,$$

$$x^3+2y^{3m}+3z^{3n}=t^3.$$

(Carmichael, 1913.)

39. Show how to find r rational numbers such that if a given number is added to their sum or to the sum of any $r-1$ of them the results shall all be squares. (Holm, Cunningham, Wallis, 1906.)

40. Find several cubes such that the sum of the divisors of each is a square. (Fermat.)

41. Find several squares such that the sum of the divisors of each is a cube. (Fermat.)

42. Prove that 25 is the only square which is 2 less than a cube. Prove that 4 and 121 are the only squares each of which is four less than a cube. (Fermat.)

43. Show how to determine an unlimited number of Pythagorean triangles having the same area. (Fermat.)

44. Prove that the number $2(x^2+xy+y^2)$ cannot be a square when x and y are rational. (Fermat.)

45. Prove that the equation $x^2-2=m(y^2+2)$ has no solution in positive integers m, x, y. (Fermat.)

46.* Prove that the equation $2x^2-1=(2y^2-1)^2$ has the unique solution $x=5$, $y=2$. (Fermat; Pepin, 1884.)

47. Obtain solutions of the system $x+y=u^2$, $x^2+y^2=v^4$. (Euler.)

48. Find six fifth-power numbers whose sum is a fifth power. (Martin, 1898.)

49. Find a sum of sixth-power numbers whose sum is a sixth power. (Martin, 1912.)

50.† Find a set of powers of higher degree than the sixth such that their sum is a power of the same degree. (Compare papers referred to in § 20.)

51. Solve each of the Diophantine equations $xy=z(x+y)$, $z^2(x^2+y^2)=(xy)^2$. (Mathesis (4) 3: 119.)

52. Obtain a solution of the Diophantine system $x^2+y^2+z^2=u^2$, $x^3+y^3+z^3=v^3$. (Martin and Davis, 1898.)

53. Apply the following identities to the solution of Diophantine equations:

$$(a^2-b^2)^8+(a^2+b^2)^8+(2ab)^8=2(a^8+14a^4b^4+b^8)^2,$$

$$x^8+y^8+(x^2\pm y^2)^4=2(x^4\pm x^2y^2+y^4)^2.$$

(Barisien, Visschers, 1911.)

54.* Obtain the general solution of the equation

$$x_1^2+x_2^2+\ldots+x_n^2=xx_1x_2\ldots x_n.$$ (Hurwitz, 1907.)

55. Show how to obtain solutions of the system

$$x^2+y^2+2z^2=\square,\quad x^2+2y^2+z^2=\square,\quad 2x^2+y^2+z^2=\square.$$ (Legendre.)

56. Show how to obtain solutions of the system $x^2+y^2-z^2=\square$, $x^2-y^2+z^2=\square$, $-x^2+y^2+z^2=\square$. (Legendre.)

57.* Develop a theory of the Diophantine system

$$a=x^2+y^2+u^2+v^2,$$
$$b=x+y+u+v.$$

Apply the results to several problems in the theory of numbers. (Cauchy, Legendre.)

58.* Investigate the solutions of the equation

$$x^3+(x+r)^3+(x+2r)^3+\ldots+[x+(n-1)r]^3=y^3.$$

(Genocchi, 1865.)

59. Determine systems of four numbers such that the sum of every two in a system shall be a cube. (Fermat.)

60.* Develop a general theory of the equation $(n+4)x^2-ny^2=4$. (Realis, 1883.)

61.* Determine properties of the integers a, b, c, d such that the equation $ax^2+by^2+cz^2+du^2=0$ shall have integral solutions. (Meyer, 1884.)

62.* Show how to write the product of two sums of eight squares as a sum of eight squares. (Thomson, 1877.)

63.† Develop the theory of the Diophantine equation

$$\frac{1}{x_1}+\frac{1}{x_2}+\ldots+\frac{1}{x_n}=1,$$

where $x_1, x_2, \ldots, x_n$ are restricted to be positive integers. In particular show that the maximum value of an x which can occur in a solution is u_n where $u_{k+1}=u_k(u_k+1)$ and $u_1=1$ and find the other integers which go to make up a

solution containing this number u_n. (Problem and result communicated to the author by O. D. Kellogg.)

64.† Develop a theory of the system

$$x_1+x_2+\ldots+x_n=y_1+y_2+\ldots+y_n,$$

$$x_1^2+x_2^2+\ldots+x_n^2=y_1^2+y_2^2+\ldots+y_n^2.$$

Generalize the results by adding further similar equations with exponents 3, 4, . . . (Longchamps, 1889; Frolov, 1889; Aubry, 1914.)

65.† Observe that

$$4\frac{x^3+y^3}{x+y}=(x+y)^2+3(x-y)^2$$

and thence show how to extend the set of numbers of the form $(x^3+y^3)/(x+y)$ by generalization of variables so as to form a domain with respect to multiplication. Treat likewise the forms $(x^5+y^5)/(x+y)$, $(x^7+y^7)/(x+y)$. Generalize to the form $(x^p+y^p)/(x+y)$, where p is any odd prime. (Compare Bachmann's *Zahlentheorie*, III, p. 206.)

66.† Apply the results obtained in Exercise 65 to the solution of problems in Diophantine analysis.

67.† Develop the theory of the equation $x^4+y^4=mz^2$ for given values of m. (See examples of solutions in *Interméd. d. Math.*, Vol. XVIII, p. 45.)

68.† Develop the theory of the equation $x^n+y^n+z^n=u^n+v^n$ for various values of the positive integral exponent n. (Gérardin, 1910.)

69.† Equations of the form

$$x^m=y^n+c, \tag{1}$$

where c is a given number, have been investigated by several writers. In particular, the case $c=1$ has been treated in several papers, the only known solution for the latter case (in which m and n are greater than unity) being $x=3$, $m=2$, $y=2$, $n=3$. Investigate the general theory of Eq. (1), summarizing the results in the literature and adding to them. In particular, determine whether other consecutive integers than 8 and 9 can be perfect powers. (See Proc. Lond. Math. Soc. (2) 13 (1914): 60–80.)

70.† Determine whether the sum either of n nth powers or of $n-1$ nth powers can itself be an nth power when n is greater than 3.

71.* The equation

$$q^r F\left(\frac{p}{q}\right)=c,$$

in which $F(x)$ denotes an irreducible polynomial in x of degree r $(r>2)$ with integral coefficients and c is an integer, has only a finite number of solutions in integers p and q. (Thue, 1908.)

INDEX

Abel, 90
Abelian Formulæ, 87–90
Aubry, 83, 84, 113, 116
Avillez, 52

Bachmann, 116
Barbette, 85
Barisien, 115
Bernstein, 102
Binet, 65
Biquadratic Equations, 44–48, 74–84

Carlini, 102
Carmichael, 30, 39, 42, 83, 88, 91, 114
Catalan, 52
Cauchy, 5, 100, 115
Cubic Equations, 55–73
Cunningham, 114

Davis, 52, 115
Delannoy, 72
Desboves, 112, 114
Descent, Infinite; *see* Infinite Descent
Development of Method, 6–8
Dickson, 99
Diophantine Equation, Definition of, 1
Diophantine System, Definition of, 1
Diophantus, 4, 5, 9, 104, 106, 107, 108, 111, 112, 113
Dirichlet, 5
Domain, Multiplicative, 24–54
Double Equations, 78, 107

Eisenstein, 5
Equation of Pell, 26–34
Equations, Double, 78, 107
Equations, Functional, 104–111
Equations, Triple, 107
Equations of Fourth Degree, 44–48 74–84
Equations of Higher Degree, 85–103
Equations of Second Degree, 1–44
Equations of Third Degree, 55–73
Euclid, 9
Euler, 5, 22, 65, 68, 80, 82, 112
Evans, 113

Fauquembergue, 83
Fermat, 5, 6, 7, 9, 14, 39, 60, 74, 77, 78, 86, 88, 104, 106, 107, 108, 114, 115
Fermat Problem, 86–103
Fermat's Last Theorem, 86
Fleck, 103
Frolov, 116
Fujiwara, 65
Functional Equations, Method of, 104–111
Furtwängler, 101, 102

Gauss, 5
Genocchi, 115
Gérardin, 116
Gerono, 72, 112

Haentzschel, 62
Hart, 112
Hayashi, 103
Hecke, 102
Hillyer, 23
Historical Remarks, 4–8, 9

Holm, 114
Holmboe, 90
Hurwitz, 102, 115

Infinite Descent, Method of, 14, 18–22
Integral Solution, 2

Jacobi, 5
Jonquières, 112

Kapferer, 103
Kellogg, 115, 116
Kummer, 100, 101

Lagrange, 50
Lebesgue, 52
Legendre, 50, 73, 90, 99, 112, 115
Lehmer, 13
Lind, 102
Liouville, 102
Longchamps, 116
Lucas, 6, 52, 53, 112

Maillet, 99, 103, 114
Martin, 52, 81, 85, 113, 114, 115
Mathews, 5
Method, Development of, 6–8
Method of Functional Equations, 104–111
Method of Infinite Descent, 14, 18–22
Method of Multiplicative Domain, 24–54
Meyer, 115
Meyl, 112
Miot, 113
Mirimanoff, 99, 101, 102
Moret-Blanc, 83
Moureaux, 52
Multiplicative Domain, 24–54

Paraira, 84
Pell Equation, 26–34
Pepin, 53, 80, 83, 112, 114
Pietrocola, 83
Plato, 9
Primitive Solution, 2
Pythagoras, 8, 9
Pythagorean Triangles; *see* Triangles

Quadratic Equations, 1–44

Rational Solution, 2
Rational Triangles; *see* Triangles
Realis, 44, 73, 115

Schaewen, 59
Schwering, 65
Smith, 100
Solution of Diophantine Equation, 2
Solution, Integral, 2
Solution, Primitive, 2
Solution, Rational, 2
Störmer, 114
Swinden, 113

Thomson, 115
Thue, 53, 116
Triangles, Numerical, 8
Triangles, Primitive, 8
Triangles, Pythagorean, 8, 9–11, 17, 21 22, 33, 77, 80, 103, 112, 113
Triangles, Rational, 8–13
Triple Equation, 107

Valroff, 112
Vandiver, 101, 102
Visschers, 115

Wallis, 114
Welmin, 113, 114
Werebrüssov, 53, 72
Whitford, 33
Wieferich, 101

C0-DAL-726